UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERIA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACION PARA EL CENTRO DE INFORMATICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD NACIONAL DE PIURA, PERIODO 2015-2018

Presentada por:

JHON PAUL SANDOVAL QUINO

TESIS PARA OPTAR EL TÍTULO DE

INGENIERO INFORMÁTICO

Piura, Perú

2017

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERIA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACION PARA EL CENTRO DE INFORMATICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD NACIONAL DE PIURA, PERIODO 2015-2018

LOS SUSCRITOS DECLARAMOS QUE LA PRESENTE TESIS ES ORIGINAL EN SU CONTENIDO Y FORMA:

Ing. Persi Williansh Cabrera Antón.
Asesor

Bach. Jhon Paul Sandoval Quino.
Tesista

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERIA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACION PARA EL CENTRO DE INFORMATICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD NACIONAL DE PIURA, PERIODO 2015-2018

APROBADA EN CONTENIDO Y ESTILO POR:

Dr. HUGO VICTOR ROSALES GARCÍA
PRESIDENTE- JURADO CALIFICADOR

Mgr. PEDRO CRIOLLO GONZALES
VOCAL – JURADO CALIFICADOR

Mgr. HECTOR FIESTAS BANCAYÁN
SECRETARIO – JURADO CALIFICADOR

UNIVERSIDAD NACIONAL DE PIURA
FACULTAD DE INGENIERIA INDUSTRIAL
DECANATO

ACTA DE SUSTENTACIÓN DE TESIS

Los Miembros del Jurado Calificador de la Tesis denominada: **«DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD NACIONAL DE PIURA. PERIODO 2015-2018»,** presentado por **JHON PAUL SANDOVAL QUINO,** Bachiller de la Escuela Profesional en **INGENIERÍA INFORMÁTICA**, asesorado por el **MBA. PERSI WILLIANSH CABRERA ANTÓN;** reunidos para la sustentación de ésta y luego de escuchar su exposición y las respuestas a las preguntas formuladas, la declaran:

FACULTAD DE INGENIERÍA INDUSTRIAL Dirección de Investigación UNP

Con el Calificativo: APROBADO

BUENO

En consecuencia el sustentante se encuentra **apto** para recibir el título profesional de **INGENIERO INFORMÁTICO**, conforme a Ley.

Piura, 28 de Agosto del 2017

Dr. HUGO VÍCTOR ROSALES GARCÍA
PRESIDENTE – JURADO CALIFICADOR

MSc. PEDRO ANTONIO CRIOLLO GONZALES
VOCAL – JURADO CALIFICADOR

MSc. HÉCTOR WILMER FIESTAS BANCAYÁN
SECRETARIO – JURADO CALIFICADOR

DEDICATORIA

A mi familia por su apoyo y comprensión, así como también a los que ya no se encuentran conmigo en esta vida como mis abuelos.

A mi amor Flor que siempre estuvo conmigo en todo momento.

AGRADECIMIENTO

Agradezco a Dios por brindarme la oportunidad de tener estudios, salud y perseverancia para culminar este proyecto.

A mis padres por su apoyo moral y económico, a los Ingenieros de la Facultad por los conocimientos durante mi carrera universitaria, amigos de universidad, compañeros de trabajo por su gran amistad.

RESUMEN

El contenido de esta tesis ayudará a las organizaciones y/o empresas ya sean grandes o pequeñas a tener una concienciación permanente de mantener seguros sus activos, teniendo en cuenta que la palabra activo son todos los recursos informáticos o relacionados con este para que la organización funcione correctamente y alcance los objetivos propuestos.

Se aplica la metodología MAGERIT, Metodología de Análisis y Gestión de Riesgos de las Tecnologías de la Información, la cual abarca dos procesos que son estructurados de la siguiente manera: Método de Análisis de Riesgos (Identificación, Dependencias y Valoración de los activos; Identificación y Valoración de las Amenazas; Identificación y Valoración de las Salvaguardas existentes; estimación del impacto y riesgo), Proceso de Gestión de Riesgos(Toma de decisiones y Plan de Mitigación); la herramienta Pilar, Procedimiento Informático Lógico de Análisis de Riesgos, aplicación desarrollada en java y desarrollada a medida para la implementación de Magerit.

Al finalizar se obtiene un resultado realista del riesgo que posee la organización, a partir de esto se Diseña un Plan de Seguridad aplicando políticas tanto en la seguridad física, seguridad lógica y seguridad en redes; así como también un Plan de recuperación ante un desastre y respaldo de la información.

Palabras Claves: Activos, Magerit, Análisis de Riesgo, Plan de Seguridad, Seguridad física, Seguridad lógica, Seguridad en redes, Plan de recuperación.

ABSTRACT

The content of this thesis is available in companies and / or companies and whether large or small to have a permanent awareness of maintaining their assets secure, bearing in mind that the active word all computer or related resources for the organization functions properly and Reach the proposed objectives.

The methodology MAGERIT, Methodology of Analysis and Management of Risks of Information Technologies is applied, which covers the processes that are structured as follows: Risk Analysis Method (Identification, Dependencies and Asset Valuation; Identification and Assessment of Threats; Identification and Evaluation of Existing Safeguards; Impact and risk estimation), Risk Management Process (Decision-making and Mitigation Plan), The Pillar tool, Logical Computer Procedure of Risk Analysis, an application developed in Java and developed to measure for the implementation of Magerit.

At the end a realistic result of the risk that the organization possesses is obtained, based on this, a Security Plan is designed applying policies, as well as a Disaster Recovery Plan and information backup.

Key Words: Active, Magerit, Risk Analysis, Security Plan, Physical Security, Logical Security, Network Security, Recovery Plan.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

ÍNDICE DE ANEXOS

INTRODUCCION

La información es hoy en día uno de los activos más importantes con los que cuenta cualquier empresa; un activo que no siempre tiene la consideración e importancia necesaria dentro de algunas empresas, son múltiples los riesgos asociados a que equipos, sistemas de información y comunicaciones no cuenten con controles de seguridad.

Las amenazas en las Tecnologías de Información y Telecomunicaciones (TIC) son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

El presente trabajo de investigación se desarrolla en base al Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura(UNP), el cual es un órgano de gestión encargado de las actividades informáticas y tecnológicas de la información de dicha Universidad, siendo esta última una Institución de prestigio en la Zona Norte del Perú, específicamente en el Departamento de Piura y la cual no posee una total seguridad de su información, en la cual se tendrá que detectar las deficiencias y poder aplicar control sobre ellas para evitar riesgos que puedan originar un declive en la UNP

Este trabajo "Diseño de un Plan de Seguridad de la Información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, periodo 2015-2018", estará apoyado en la norma y/o estándar internacional ISO 17799 referente a tecnología de la información, el cual expondrá la importancia que tiene la seguridad de la información dentro del CIT, además de asegurar la confidencialidad, integridad y disponibilidad de la información vital corporativa y así evitar sufrir amenazas de fuentes externas.

CAPITULO I.- EL PROBLEMA DE INVESTIGACIÓN

1.1 Descripción de la Realidad Problemática

Las tecnologías de hoy en día poseen información que es considerado un activo cada vez más valioso el cual puede hacer que una organización triunfe o quiebre, es por eso que debemos brindarle seguridad.

Existe una realidad que no favorece a la Universidad Nacional de Piura a la que luego denominaré UNP en donde el problema es que el Centro de Informática y Telecomunicaciones (CIT) no posee una total seguridad de sus activos informáticos (son aquellos recursos, hardware, software, datos, información, equipos de telecomunicación; con los que cuenta la Institución), como consecuencia se tendrá una exposición de la información que posee, ocasionando con el pasar del tiempo diferentes riesgos que ocasionarán un impacto negativo en la UNP.

El motivo de no poseer total seguridad de los activos informáticos es que la Universidad desconoce la magnitud del problema con el que se enfrentan considerando la seguridad como algo secundario; por lo tanto no se invierte capital humano ni económico necesario para prevenir el daño y/o pérdida de la información que hoy en día con el uso de nuevas tecnologías para almacenarla, transmitirla y recobrarla está expuesta; esto se debe a la falta de compromiso de nuestras autoridades que no le toman la importancia que se merece.

De continuar la situación, se puede pronosticar un robo permanente de la información así como la existencia de distintas amenazas las cuales afectarán características principales de la seguridad como son la confidencialidad, integridad y disponibilidad de la información que pueden ser internas o externas, originadas accidentalmente o con un fin perverso dejando a la organización con problemas, como por ejemplo: la paralización de sus actividades ,que deja como resultado una pérdida cuantiosa de tiempo de producción y un malestar por parte de la comunidad universitaria, lo que provocaría un declive en el desarrollo de este órgano de gestión.

En la actualidad son muchos los riesgos que pueden afectar la seguridad de información de este órgano de gestión y por lo general como el capital con el que se cuenta para protegerlo no es suficiente, debemos tener identificadas y controladas estas vulnerabilidades, esto se logra con un adecuado plan de seguridad elaborado en base a un análisis de riesgo previo.

Por ende, se debe plantear un control ante tal situación en el cual se propondrá el trabajo Plan de Seguridad de la Información en el Centro de Informática y Telecomunicaciones de la UNP a fin de alcanzar la eficiencia y eficacia en las actividades de resguardo o protección de los activos informáticos.

1.2 Delimitación de la Investigación

1.2.1 Delimitación Espacial

El ámbito en el cual se desarrollará el proyecto de Investigación comprende a la Universidad Nacional de Piura, ubicada en el Distrito de Castilla, que pertenece a la Provincia de Piura, Departamento de Piura.

1.2.2 Delimitación Social

El presente proyecto se Implementará para que la Universidad Nacional mantenga segura su información y sus equipos tecnológicos. Está orientado además a brindar un mejor servicio a la Universidad.

1.2.3 Delimitación Temporal

El presente Proyecto de Investigación se llevará a cabo desde el mes de Agosto hasta Diciembre del presente año 2016 para lo cual se tendrá que recopilar los datos necesarios para su conclusión.

1.2.4 Delimitación Conceptual

La investigación abarcará los temas: Seguridad de la Información, Seguridad Informática, Análisis de Riesgos, Arquitectura de la Seguridad, Normas y Estándares Internacionales. Los cuáles serán desarrollados en el marco teórico.

1.3 Formulación del Problema

¿Es posible que el plan de seguridad de la información en el Centro de Informática y Telecomunicaciones ayude a mejorar la protección de los activos informáticos?

1.4 Objetivos de la Investigación

1.4.1 Objetivo General

Diseñar un plan de seguridad de la información para proteger los activos informáticos que se utilizan y generan en los procesos de la Universidad administrados por el Centro de Informática y Telecomunicaciones.

1.4.2 Objetivos Específicos

- Diagnosticar la seguridad que se desarrolla en el CIT.

- Determinar los riesgos que afectan la seguridad de información, identificando las vulnerabilidades y amenazas a los que se enfrenta el CIT.

- Diseñar un modelo de seguridad aplicando la norma y/o estándar de seguridad de la información ISO 17799.

1.5 Hipótesis y Variables de la Investigación

1.5.1 Hipótesis General

El Diseño de un Plan de seguridad de la información ayudará a mejorar la seguridad de los activos informáticos que se utilizan y generan en cada uno de los procesos de la UNP.

1.5.2 Variables

- Variable Independiente (X):

  Diseño de un Plan de seguridad de la información para el Centro de Informática y Telecomunicaciones

- Variable Dependiente(Y):

  Seguridad de activos informáticos.

1.5.2.1 Operacionalidad de las Variables

1.5.2.1.1 Variable Independiente (X)

- Tiempo de resguardo de la información.

- Porcentaje de evaluación de riesgos de seguridad identificados y evaluados con niveles de importancia alta, media o baja.

- Nivel de aplicación de políticas de seguridad en la organización.

- Número de incidentes de seguridad de red identificados en los meses anteriores, dividido por categorías de leve, importante y grave importancia.

- Número de peticiones de cambios de acceso por parte del personal que labora en la institución.

- Cantidad de equipos protegidos y vulnerables, es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (laptops, teléfonos móviles, etc.).

- Frecuencia de aplicación de los controles de validación de datos que se han definido e implementado, demostrándose eficaces mediante pruebas.

- Frecuencia de sistemas evaluados del CIT de forma independiente conforme a estándares de seguridad básica.

1.5.2.1.2 Variable Dependiente (Y)

- Nivel de satisfacción de empleados.

- Porcentaje de empleados que han recibido y aceptado formalmente, roles y responsabilidades con respecto a seguridad de la información.

- Número de informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización.

- Número y costes acumulados de incidentes por software malicioso como virus, gusanos, troyanos o spam detectados y bloqueados.

- Frecuencia de backups de archivos con datos sensibles o valiosos que se encuentran protegidos dentro y fuera de la empresa.

- Número de incidentes de la seguridad en los procesos de desarrollo de software.

- Número de chequeos (a personas a la salida) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.

- Porcentaje de nuevos empleados relacionados con las tecnologías de información y comunicaciones (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la institución antes de comenzar a trabajar.

1.5.3 Indicadores

ITEM	INDICADOR	DEFINICION CONCEPTUAL	CANTIDAD	CALIDAD	TIEMPO
I1	Aplicación de estándares de seguridad en la organización.	Es el número de estándares que se aplicará para el resguardo de la información de la organización.	Se aplicará entre 1 a 3 estándares según cada proceso de la organización.	Protección de los activos informáticos de la organización.	De manera trimestral.
I2	Número de incidencias de información expuesta.	Es la cantidad de veces que ha estado expuesta la información.	Número de incidentes de seguridad identificados < 50 incidencias.	Mejorar el resguardo de la información de la organización.	De manera bimestral.
I3	Nivel de satisfacción de empleados.	Es la medida de nivel de satisfacción hacia el plan desde la perspectiva del empleado.	Número de peticiones de cambios de acceso < 5 peticiones por área.	Crear en los empleados una cultura de seguridad Informática.	De manera trimestral.

Tabla 1: Indicadores

1.5.4 Tipo y Nivel de la Investigación

Este trabajo se considera una Investigación Aplicada Fundamental, ya que es de vital importancia el desarrollo de un Plan de Seguridad dentro del Órgano encargado de los Sistemas y Tecnología de la Universidad para la protección de los Sistemas y Aplicativos implementados para el uso de la comunidad universitaria.

El nivel de la investigación es de tipo descriptiva, para conocer con mayor profundidad las circunstancias en las que se produce el problema y la realidad en la que se desarrolla.

Conoceremos las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas.

1.5.5 Método de la Investigación

Se empleará el método analítico-sintético ya que se estudia los hechos, partiendo de la descomposición del objeto de estudio en cada una de sus partes para estudiarlas en forma individual (análisis) y luego se integran dichas partes para estudiarlas de manera holística e integral (síntesis).

1.5.6 Población y Muestra de la Investigación

1.5.6.1 Población

La población en estudio está conformada por 38 usuarios Administrativos que laboran en el Centro de Informática y Telecomunicaciones de la UNP que utilizan equipos informáticos.

.

1.5.6.2 Muestra

Debido a que la muestra del sector de usuarios que laboran con un equipo informático es muy pequeña se vio por conveniente aplicar la técnica de muestreo aleatorio simple, la cual se determina a continuación:

$$n = \frac{N\ Z^2\ P\ Q}{Z^2\ P\ Q + (N-1)E^2}$$

Dónde:

Z = Abscisa de la distribución normal estándar según nivel de confianza al 95%, establecido por el investigador (**Z**=1.96)

P = Proporción que posee la característica en estudio (**P**=0.50)

Q =Proporción que no posee la característica en estudio (**Q**=0.50)

E = Estimación de error (**E**=0.05)

N = Población o Universo (**N**=38)

n = Tamaño de muestra.

Cálculo del Tamaño de Muestra:

$$n = \frac{(38)1.96^2\ (0.50)(1-0.50)}{1.96^2\ (0.50)(0.50) + (37)(0.05)^2}$$

$$n = 34.661$$

$$n = 35.$$

1.5.7 Justificación, importancia y Limitaciones

a) Justificación

La información y los procesos son activos comerciales importantes, la confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener una ventaja competitiva, rentabilidad, conformidad legal e imagen comercial

La necesidad de esta investigación es proteger los activos Informáticos del CIT, contra las variedades de amenazas; identificar los riesgos a los que se encuentra expuesta la información, diseñar correctivos apropiados basados en políticas y estándares de seguridad que colaboren a reducir el riesgo a un nivel aceptable, proporcionar una mejora en la seguridad de los activos informáticos.

La seguridad informática tiende a ser motivo de descuido en las empresas, si no se describen los puntos importantes en su estudio, se ignora de los riesgos que conlleva confiar la información a los sistemas de información.

b) Importancia

Es importante ya que así se conoce la problemática que puede traer el no conocer los aspectos que pueden evadir la seguridad informática en las empresas tanto físicas como lógicas.

Es necesario tener seguridad en la información ya que las organizaciones se apoyan de la informática para mantener la operación, producción y administración organizacional y es necesaria como lo menciona Maiwald "La seguridad informática es necesaria para proteger la información en tránsito"[1]

Debemos de tomar en cuenta que a la información o los sistemas de cómputo de una organización les pueden ocurrir ataques de diversas maneras, algunas de estas son hechas a propósito y otras ocurren por

[1]Maiwald (2003, P.10)

accidente. Sin importar como ocurran los eventos, es importante conocer y estudiar todas las formas de ataques y las maneras de proteger la información.

La trascendencia de este trabajo es dar a conocer lo importante que es la información para cualquier organización, debido a que sin ella dejaría de funcionar; principalmente si hablamos del CIT que es encargado de las actividades informáticas y tecnológicas de la Universidad, basta con mirar sus actividades para darnos cuenta que la seguridad es el factor más determinante para su inactividad; por lo tanto es importante ser conscientes de que por más que se piense que este órgano de gestión sea seguro, con el incremento del uso de nueva tecnología para manejar la información nos hemos abierto a un mayor número y tipos de amenazas.

Por ello es necesario que se asegure las características importantes de la información y así evitar sufrir amenazas de fuentes externas como los virus, hackers, troyanos entre otros y de fuentes internas como los originados por los empleados; por lo tanto, la seguridad de la Información siempre debe de ser tomada en cuenta.

c) Limitaciones

La falta de un área de seguridad dentro de las Instalaciones del Centro de Informática y Telecomunicaciones al momento de la Investigación

No se podrá acceder más detalladamente a la inmensa cantidad de información que se trabaja en cada uno de los procesos de la Universidad debido a que este activo es muy valioso para la Institución

CAPITULO II.- MARCO TEÓRICO

2.1 Marco Referencial

2.1.1 Centro de Informática y Telecomunicaciones

Jefe: Mg. Wilfredo Cruz Yarlequé.

Dirección: Campus Universitario, Urb. Miraflores s/n, Castilla- Piura Apartado Postal 295.

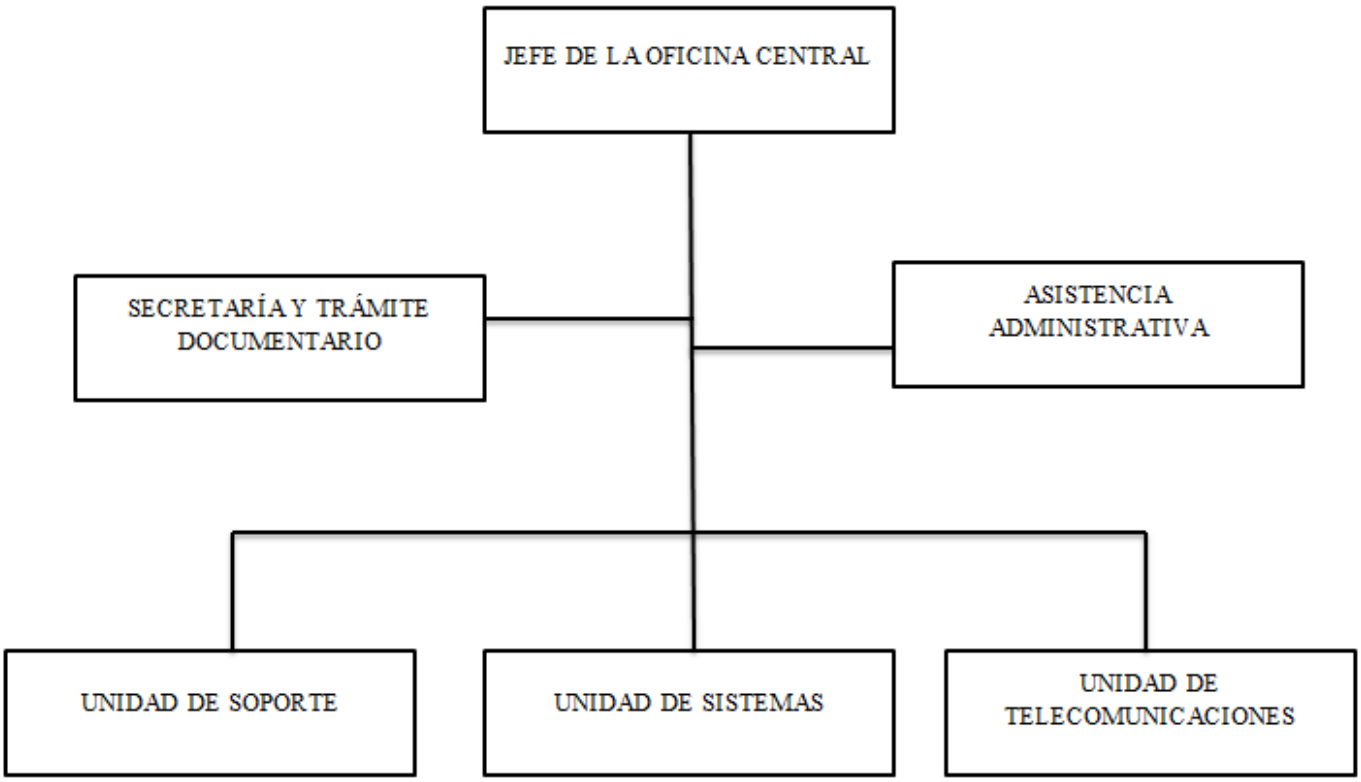


Gráfico 1: Organigrama del Centro de Informática y Telecomunicaciones de la UNP.

Fuente: Elaboración Propia

2.1.2 Introducción al CIT

El Centro de Informática y Telecomunicaciones (CIT) como órgano de gestión orientado a las actividades informáticas y tecnologías de la información, considera tres líneas de acción: **Evaluación** de la plataforma tecnológica en función a las necesidades propias de la institución, **Orientación** hacia una plataforma y uso de software libre en las unidades operativas, y: **Creación de capacidades** para el logro de las metas propuestas.

Estas acciones, tiene como objetivo continuar con la sistematización que nos permita:

a) El uso de nuevas tecnologías como facilitadoras de un proceso de cambio, innovando las formas de trabajo, rediseñando la universidad, optimizando los recursos, y mejorando la calidad del servicio

b) Crear mejores condiciones laborales, dentro de un ambiente de trabajo, propicio para que los operadores cuenten con las herramientas tecnológicas en el desarrollo de sus funciones, y le permita brindar un mejor servicio.

2.1.3 Diagnóstico

El Centro de Informática y Telecomunicaciones de la Universidad es la dependencia Central de mucha importancia en nuestra institución. Fieles y concientes a esa responsabilidad busca siempre la construcción, diseño y puesta en ejecución de Proyectos de Tecnologías de Información con el objetivo de preparar a la Universidad para los retos y cambios constantes del mundo globalizado en la que se encuentra inmersa. Proyectos a nivel de comunicaciones y conectividad es la mejor carta de presentación del carácter innovador y con responsabilidad social, que la UNP muestra para conocimiento público.

Nuestro ideal es que los alumnos posean las herramientas de la modernidad educativa y nuestros profesionales en el rubro de Tecnologías de Información sean los mejores a nivel intelectual, moral y personal en los campos de especialización en los que les toque desempeñarse. A nivel de comunidad, las herramientas informáticas se ofrecen a través del dictado de diversos cursos con el objetivo de elevar el nivel de conocimiento y preparar al estudiante para que pueda afrontar los nuevos retos de la nueva ideología mundial.

2.1.4 Apoyo en la Formación Académica

El CIT es una de las dependencias de la UNP que colabora con la formación académica de los alumnos sobre todo de las especialidades de Ingeniería Electrónica y Telecomunicaciones, así como los de Ingeniería informática y de los alumnos de la Escuela tecnológica- especialidad de Sistemas, puesto que estos alumnos recurren a éste Centro para realizar sus práctica pre-profesionales.

2.1.5 Misión y Visión

a) Misión

Conducir, administrar y velar por la integridad del parque informático, red informática, comunicación e Iso sistemas e información con otros organismos e instituciones nacionales e internacionales de su competencia. Así mismo somos los responsables de respaldo y seguridad de la información y de los sistemas de la UNP, de las necesidades de mantenimiento y servicios de equipos informáticos con alta calidad, precios justos y excelente servicio.

b) Visión

Ser la unidad líder de todo el sistema universitario de la región Grau en brindar soluciones tecnológicas idóneas que estén alineadas a los objetivos institucionales con la finalidad de satisfacer las necesidades de la institución, para ello nuestro compromiso es innovar y mejorar la calidad de servicio para satisfacción de nuestros clientes bajo lineamientos de buenas prácticas profesionales y la eficiencia de nuestro sistema de gestión de calidad

2.1.6 Áreas

El centro de Informática y Telecomunicaciones se divide en las siguientes áreas:

a) **Jefe de la Oficina Central**: Es el área que está a cargo del Director del CIT, el cual se encarga de dirigir y controlar los distintos ambientes de trabajo.
b) **Secretaría y Tramite Documentario**: Se encarga de planificar, organizar, dirigir y controlar los diversos trámites y archivo de documentos de importancia para el CIT.
c) **Asistencia Administrativa**: Es el área encargada de ejecutar los procesos administrativos del CIT de la UNP.
d) **Unidad de Sistemas**: Es el área responsable del desarrollo de soluciones informáticas para diversas unidades y departamentos que integran la Universidad.
e) **Unidad de Soporte**: Es la responsable de prestar atención preventiva y correctiva a los equipos computacionales de la Universidad.
f) **Unidad de Telecomunicaciones**: Es el área responsable de la infraestructura de la Red de datos y de los servicios de comunicaciones de la Universidad.

2.1.7 Objetivos Estratégicos-Estrategias de Impacto

a) **Objetivo estratégico 1:** Incentivo económico a practicantes para lograr mayor apoyo en la realización de las tareas

Estrategia de impacto

Darle mayor responsabilidad a los trabajos que se les encarga optimizando tiempo de respuesta y logro de objetivo.

b) **Objetivo estratégico 2:** Mayor apoyo a la capacitación de personal para enfrentar los avances tecnológicos

Estrategia de impacto

Demostrar que la tecnología se cambia diariamente y se necesita estar capacitado para afrontar esos cambios

c) **Objetivo estratégico 3:** Coordinar con los responsables de los sindicatos para que sus paralizaciones no afecten el funcionamiento de nuestro servicio

Estrategia de impacto

Buscar alternativas para evitar que las paralizaciones alteren y/o afecten el funcionamiento de esta dependencia y evitar pérdidas.

d) **Objetivo estratégico 4:** Evitar continuas interrupciones de labores que conllevan al deterioro de la imagen de nuestra universidad

Estrategia de impacto

Que las paralizaciones no perjudiquen los compromisos adquiridos y que se puedan desarrollar las actividades programadas

e) **Objetivo estratégico 5:** Mejorar el equipamiento (servidores para almacenamiento de datos) con tecnología de punta.

Estrategia de impacto

Demostrar que las necesidades en la institución crecen y los datos aumentan geométricamente y los equipos van quedando insuficientes y desfasados por el avance de la tecnología.

f) **Objetivo estratégico 6:** Lograr en el menor tiempo posible la adquisición de equipos, insumos y accesorios para una atención oportuna.

Estrategia de impacto

Demostrar el desabastecimiento de insumos, materiales y herramientas.

g) **Objetivo estratégico 7:** Contar con un grupo electrógeno de emergencia para que funcione automáticamente, evitar el deterioro de los equipos.

Estrategia de impacto

Demostrar la necesidad de contar con éste equipo para evitar la interrupción del servicio y el deterioro de los equipos.

2.2 Bases Teórico-Científicas

2.2.1 Evolución Histórica de la Seguridad

Algunos descubrimientos arqueológicos denotan con evidencias la importancia de la seguridad para las antiguas generaciones, entre estos tenemos las pirámides egipcias, el palacio de Sargon, el Dios egipcio Anubis, los Sumaricos, el Código de Hammurabi, entre otros. Hasta se dice que Julio César utilizaba esquemas de seguridad en época de guerra y en el gobierno.

Al definir el objetivo de la seguridad Fayol dice: "salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y traiciones por parte del personal, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio."

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera.

En cambio, desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

2.2.2 Seguridad de la Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones además de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma, el concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último se encarga de la seguridad en el medio

informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor, puede ser divulgada, mal utilizada, ser robada, borrada o saboteada; esto afecta su disponibilidad y la pone en riesgo. La información es poder, según las posibilidades estratégicas que ofrece tener acceso a cierta información, esta se clasifica como:

Critica: Es indispensable para la operación de la empresa

Valiosa: Es un activo de la empresa y muy valioso

Sensible: Debe de ser conocida por las personas autorizadas.

2.2.3 Seguridad Informática

La seguridad informática es la disciplina que se ocupa de diseñar las normas, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

La seguridad informática son técnicas desarrolladas para proteger los equipos informáticos y la información, de daños accidentales o intencionados. (Monografías, s.f)

2.2.3.1 Objetivo de la Seguridad Informática

La seguridad informática tiene como principal objetivo proteger el activo más importante que tiene la empresa que es su información, de los riesgos a los que está expuesta. Para que la información sea considerada confiable para la organización sus estrategias de negocio dependerán del almacenamiento, procesamiento y presentación de la misma, esta deberá cubrir los tres fundamentos básicos de seguridad para la información que son:

• **Confidencialidad:**

Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basándose en este principio, las herramientas de seguridad informática deben de proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados

•**Integridad:**

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben de asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

•Disponibilidad:

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben de reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromisos con el usuario, es prestar servicio permanente.
La seguridad informática se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial. (Garcia & Villegas, 2014)

2.2.3.2 Riesgos

Los riesgos se pueden definir como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo y según la Organización Internacional por la Normalización (ISO) define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños". Podemos concluir que cualquier problema que afecte al total funcionamiento de la empresa es considerado un riesgo o amenaza para la entidad. (Garcia & Villegas, 2014)

2.2.3.2.1 Factores de Riesgo

a) **Ambientales/Físicos:** Factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, humedad, calor entre otros

b) **Tecnológicos:** Fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informático, etc.

c) **Humanos:** Hurto, adulteración, fraude, modificación, revelación, perdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, alteraciones, etc (Vanegas M., s.f)

2.2.3.3 Evaluación de los Riesgos

Proceso por el cual se identifican las vulnerabilidades de la seguridad. El objetivo general de evaluar los riesgos será identificar las causas de los riesgos potenciales, en toda la organización, a parte de ella o a los sistemas de información individuales, a componentes específicos de sistemas o servicios donde sea factible y cuantificarlos para que la Gerencia pueda tener información suficiente al respecto y optar por el diseño e implantación de los controles correspondientes a fin de minimizar los efectos de las causas de los riesgos.

Los pasos para realizar una evaluación de riesgos se detallan a continuación:

2.2.3.3.1 Identificar los Riesgos

En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático, existen formas de identificarlos como:

- **Cuestionarios de análisis de riesgos:** La herramienta clave en la identificación de riesgos son los cuestionarios, los mismos que están diseñados para guiar al administrador de riesgos para descubrir amenazas a través de una serie de preguntas y en

algunas instancias, este instrumento está diseñado para incluir riesgos asegurables e in-asegurables.

- **Listas de chequeo de exposiciones a riesgo:** Una segunda ayuda importante en la identificación de riesgos y una de las más comunes herramientas en el análisis de riesgos son las listas de chequeo, las cuales son simplemente unas listas de exposiciones a riesgo.
- **Listas de chequeo de políticas de seguridad:** Esta herramienta incluye un catálogo de varias políticas de seguridad que un negocio dado puede necesitar. El administrador de riesgos consulta las políticas recolectadas y aplicadas a la firma.
- **Sistemas expertos:** Un sistema experto usado en la administración de riesgos incorpora los aspectos de las herramientas descritas anteriormente en una sola herramienta. La naturaleza integrada del programa permite al usuario generar propósitos escritos y prospectos.

2.2.3.3.2 Método de Análisis de Riesgos

a) **Caracterización de los activos**
   - Identificación de los activos.
   - Valoración de los activos

b) **Caracterización de las Amenazas**
   - Identificación de las amenazas.
   - Valoración de las amenazas

c) **Caracterización de las salvaguardas**
   - Identificación de las salvaguardas pertinentes.
   - Valoración de las salvaguardas

d) **Estimación del estado de riesgo:**

- Toma de decisiones.
- Plan de mitigación.

2.2.3.4 Arquitectura de Seguridad

Una arquitectura de Seguridad de la Información global y flexible implantada en toda la organización es el primer paso necesario para proteger la confidencialidad, integridad y disponibilidad de la información y los recursos del sistema, los programas de seguridad más eficaces son aquellos que cuentan con una participación activa desde dentro de la organización, fuentes externas pueden proporcionar conocimientos y experiencia específica, no obstante, el programa de seguridad en sí debe ser dirigido y gestionado internamente

La arquitectura de Seguridad es necesaria en los entornos actuales de proceso distribuido, en los que todo el mundo tanto dentro de la organización como externo a la misma tiene una responsabilidad en la seguridad de los sistemas y redes a las que tiene acceso. Los controles implantados deben incluir una combinación de procedimientos administrativos, físicos y técnicos que se seleccionan en función de los tipos de amenazas y el riesgo real estimado. (Portillo, 2010)

2.2.3.4.1 Áreas de Seguridad

A. Seguridad Lógica

La seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático. La seguridad lógica se

complementa seguridad física. La seguridad lógica de un sistema informático incluye:

- Restringir al acceso a programas y archivos mediante claves y/o encriptación.

- Asignar las limitaciones correspondientes a cada usuario del sistema informático. Esto significa, no darle más privilegios extras a un usuario, sino sólo los que necesita para realizar su trabajo.

- Asegurarse que los archivos y programas que se emplean son los correctos y se usan correctamente. Por ejemplo, el mal uso de una aplicación puede ocasionar agujeros en la seguridad de un sistema informático.

- Control de los flujos de entrada/salida de la información. Esto incluye que una determinada información llegue solamente al destino que se espera que llegue, y que la información llegue tal cual se envió. Los controles anteriormente mencionados se pueden hacer a nivel sistema operativo, a nivel aplicación, a nivel base de datos o archivo, o a nivel firmware (Alegsa, 2013)

B. Seguridad Física

La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. La seguridad física se complementa con la seguridad lógica. Los mecanismos de seguridad física deben resguardar

de amenazas producidas tanto por el hombre como por la naturaleza. Básicamente, las amenazas físicas que pueden poner en riesgo un sistema informático son:

* Desastres naturales, incendios accidentales, humedad e inundaciones.

* Amenazas ocasionadas involuntariamente por personas.

* Acciones hostiles deliberadas como robo, fraude o sabotaje.

Son ejemplos de mecanismos o acciones de seguridad física:

- Cerrar con llave el centro de cómputos.
- Tener extintores por eventuales incendios.
- Instalación de cámaras de seguridad.
- Guardia humana.
- Control permanente del sistema eléctrico, de ventilación, etc. - (Alegsa, 2010)

2.3 Normas y/o Estándares Internacionales

Todo procedimiento informático debe estar apoyado en estándares y/o normas referentes a tecnología de información, así como también una metodología para que brinden la seguridad que la organización necesita.

2.3.1 Norma ISO 17799

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio

La seguridad de la información se define como la preservación de:

- Confidencialidad: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- Integridad. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

La norma ISO 17799 establece diez dominios de control que cubren por completo la gestión de la seguridad de la información:

1. Política de seguridad.

2. Aspectos organizativos para la seguridad.

3. Clasificación y control de activos.

4. Seguridad ligada al personal.

5. Seguridad física y del entorno.

6. Gestión de comunicaciones y operaciones.

7. Control de accesos.

8. Desarrollo y mantenimiento de sistemas.

9. Gestión de continuidad del negocio.

10. Conformidad con la legislación.

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

(Villalon Huerta, 2004)

2.4 Antecedentes del Problema

2.4.1 Antecedentes Latinoamericanos

Hernández Pinto María (2006), en su trabajo de tesis planteó Diseñar un Plan Estratégico de Seguridad de Información en una empresa del sector comercial, el desarrollo de este trabajo ayudará a las organizaciones comerciales a tener una permanente seguridad de sus activos, teniendo en cuenta que la palabra activo son todos los recursos informáticos o relacionados con éste para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección, además de esto se da a conocer la importancia, valor, razones de vulnerabilidades y vulnerabilidades de la información para formarnos un criterio del por qué es necesario mantener la seguridad en los activos informáticos, las principales conclusiones que se llevaron a cabo fueron: Las herramientas de tecnología evolucionan con el pasar del tiempo volviéndose inseguras en la medida que su utilización no sea la más adecuada en la organización, convirtiéndose así

en objeto de amenazas. Hoy en día en toda empresa es una necesidad más frecuente utilizar esquemas de seguridad fuertes, que permitan una mayor confiabilidad de la información utilizada para la toma de decisiones, la seguridad de la información es una responsabilidad compartida de todos los niveles de la organización, que requiere del apoyo de todos ellos pero debe estar dirigida por un plan y con la adecuada coordinación. El motivo por la cual fue considerada esta investigación es debido a que se encuentra orientada a la protección de la información tanto de manera física como lógica bridando un plan estratégico de seguridad de información al sector comercial.

DOLORES,M e IGNACIO,P (2002); se diseñó para el departamento de sistemas de la empresa Fabril Fame con la finalidad de proteger los recursos informáticos y asegurar la viabilidad de las operaciones,en este proyecto se refleja una visión de alto nivel de los requerimientos de información de la organización FAME S.A., y se desarrolla una planificación para satisfacer dichos requerimientos mediante el levantamiento de información a los usuarios en las áreas de los procesos claves, a través de entrevistas y observación. Para este desarrollo se aplica el marco de trabajo PETI (Planificación Estratégica de Tecnologías de Información), que permite el entendimiento administrativo de la empresa para desarrollar las estrategias de tecnologías de información que impulsen las estrategias de negocio, se identificó las falencias existentes y puntos críticos de la organización para luego plantear soluciones tecnológicas y reducir el impacto de estas falencias teniendo como consecuencia que la empresa FAME S.A cumpla con sus objetivos empresariales. El motivo por el cual fue considerado este trabajo; es debido a la similitud que tiene con este proyecto de investigación que se está llevando a cabo.

2.4.2 Antecedentes Nacionales

Córdova Rodríguez Norma (2003), El objetivo principal de esta autora es realizar un diagnóstico de la situación actual en cuanto a la seguridad de

información que el Banco ABC actualmente administra y diseñar un Plan de Seguridad de la Información (PSI) que permita desarrollar operaciones seguras basadas en políticas y estándares claros y conocidos por todo el personal del Banco,empezando por definir la estructura organizacional (roles y funciones), después pasa a definir las políticas, para finalmente concluir con un plan de implementación o adecuación a las políticas anteriormente definidas.Las principales conclusiones de esta investigación son: La clave para desarrollar con éxito un programa efectivo de seguridad de la información consiste en recordar que las políticas, estándares y procedimientos de seguridad de la información son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica. Muchas organizaciones ignoran esta interrelación en un esfuerzo por simplificar el proceso de desarrollo. Sin embargo, estas mismas relaciones son las que permiten que las organizaciones exijan y cumplan los requerimientos de seguridad. Este tema de investigación nos permite tener un conocimiento más amplio de la seguridad, que se regirá bajo normas para el adecuado uso de la información dentro y fuera de la organización siendo está muy importante dentro de la misma.

2.5 Definiciones Conceptuales

2.5.1 Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

2.5.2 Amenaza

Cualquier evento que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

2.5.3 Análisis de riesgo

Es el estudio de las posibles amenazas y probables eventos no deseados es decir los daños y consecuencias que éstas puedan producir.

2.5.4 Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

2.5.5 Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o Tablas de bits), vídeo (secuencia de tramas), etc.

2.5.6 Base de Datos

Cualquier conjunto de datos organizados para su almacenamiento en la memoria de un ordenador o computadora, diseñado para facilitar su mantenimiento y acceso de una forma estándar. Los datos suelen aparecer en forma de texto, números o gráficos.

2.5.7 Controles

Comprende los métodos, sistemas y procedimientos, que, en forma ordenada, se adoptan en una organización, para asegurar la protección de todos sus recursos.

2.5.8 Riesgo

Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

2.5.9 Hardware

Equipo utilizado para el funcionamiento de una computadora. El hardware se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento.

2.5.10 Software

Conjunto de programas de computadoras. Son las instrucciones responsables de que el hardware (la máquina) realice su tarea.

2.5.11 Seguridad Informática

Son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

2.5.12 Seguridad de la información

Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

2.5.13 Virus (informática)

Son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de "inmunizar" o eliminar el virus del ordenador.

2.5.14 Vulnerabilidad

Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.

Capitulo III.- MARCO METODOLÓGICO

3.1 Metodología

Para el desarrollo del presente proyecto se empleará la metodología Magerit Versión 3.0.

3.1.1 Magerit Versión 3.0

La Metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

a) Finalidad:

El análisis y gestión de los riesgos es un aspecto clave del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica que tiene la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información

b) Objetivos:

MAGERIT persigue los siguientes objetivos:

Directos:

Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos

c) Descripción:

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

MAGERIT permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

d) Organización de las guías

MAGERIT versión 3 se ha estructurado en tres guías:

i. Método:

Se estructura de la siguiente forma:

- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.
- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

ii. Catálogo de Elementos

Marca unas pautas en cuanto a:

- tipos de activos.
- dimensiones de valoración de los activos.
- criterios de valoración de los activos.
- amenazas típicas sobre los sistemas de información.
- salvaguardas a considerar para proteger sistemas de información.

Se persiguen dos objetivos:

- Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
- Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Cada sección incluye una notación XML que se empleará para publicar regularmente los elementos en un formato estándar capaz de ser procesado automáticamente por herramientas de análisis y gestión.

Si el lector usa una herramienta de análisis y gestión de riesgos, este catálogo será parte de la misma; si el análisis se realiza manualmente, este catálogo proporciona una amplia base de partida para avanzar rápidamente sin distracciones ni olvidos.

iii. Guía de Técnicas

Aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

❖ **Técnicas específicas para el análisis de riesgos**

- análisis mediante tablas.
- análisis algorítmico.
- árboles de ataque.

❖ **Técnicas específicas para el análisis de riesgos**

- técnicas gráficas.

- sesiones de trabajo: entrevistas, reuniones y presentaciones.
- valoración Delphi.

Se trata de una guía de consulta. Según el lector avance por las tareas del proyecto, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

e. Ventajas:

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. (Portal de Administración Electrónica, 2012)

3.2 Cobertura de Estudio

El presente proyecto está dirigido a los 38 usuarios administrativos que laboran en el Centro de Informática y Telecomunicaciones de la UNP que utilizan equipos informáticos.

3.3 Técnicas e instrumentos de recolección de datos

Para ello se utilizará la herramienta Pilar en su versión 5.4.7, el software Microsoft Excel.

3.3.1 Herramienta PILAR 5.4.7

Procedimiento Informático Lógico de Análisis de Riesgos, PILAR, es una aplicación implementada en java basada en la metodología MAGERIT, desarrollada por el Centro Criptológico Nacional y con un gran calado en la administración pública española. La versión vigente es la 5.4.7. Su licencia de prueba es de 30 días, no obstante, para uso en entorno privado dicha licencia tiene un coste. La herramienta permite la realización de análisis de riesgos bajo un enfoque tanto cualitativo como cuantitativo (empleando valores simbólicos o económicos respectivamente) y la realización de análisis de impacto en el ámbito de la continuidad de negocio.

a) Análisis y Gestión de Riesgos

Se analizan los riesgos en varias dimensiones

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad

Para tratar el riesgo se proponen:

- Salvaguardas (o contramedidas)
- Normas de seguridad
- Procedimientos de seguridad

Analizándose el riesgo residual a lo largo de diversas etapas de tratamiento

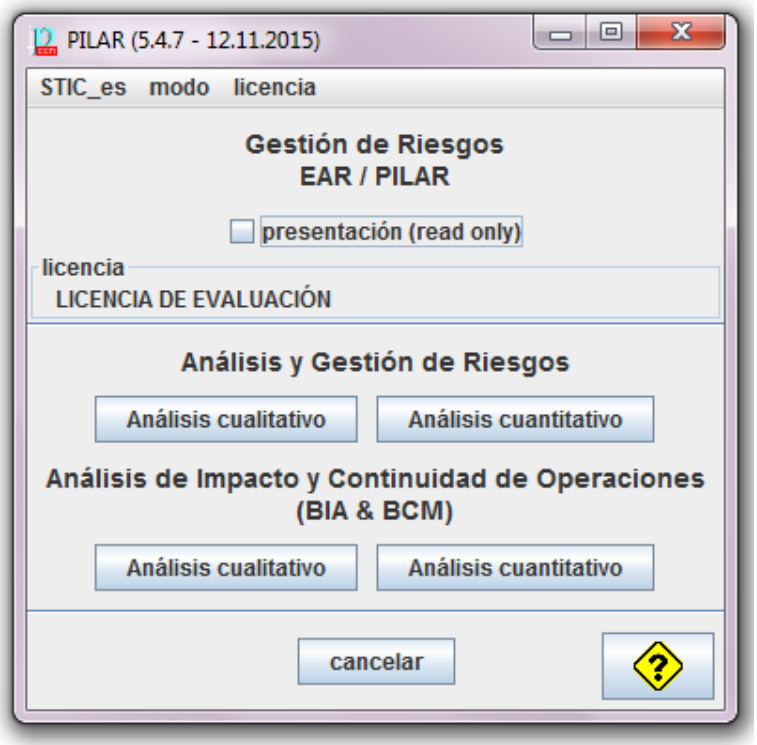


Gráfico 2: Herramienta Pilar- Pantalla Principal
Fuente: Herramienta Pilar en su versión 5.4.7

Para la utilización de la herramienta PILAR, es necesario disponer de una licencia de uso, en el caso del presente proyecto se solicitó una licencia de evaluación de 30 días.

CAPÍTULO VI. - DESARROLLO DE LA PROPUESTA DE INVESTIGACIÓN

4.1 Equipo de Trabajo

Este trabajo será realizado por dos personas; quien está redactando Jhon Paul Sandoval Quino dirigido por el Asesor de Tesis Persi Williansh Cabrera Antón.

4.2 Descripción del Entorno Informático

El Centro de Informática y Telecomunicaciones cuenta con 5 áreas: Jefe de la Oficina Central, Secretaría y Trámite Documentario, Asistencia Administrativa, Unidad de Soporte, Unidad de Sistemas, Unidad de Telecomunicaciones; las cuales están integrados por el director del CIT y empleadores administrativos, así como también practicantes; estas personas tienen las siguientes funciones según el rol que desempeñan dentro de cada área.

Jefe de Oficina Central:

- Administrar los recursos del área.
- Control y mantenimiento de la red y programas que dan servicio a la institución.
- Gestión de las adquisiciones de equipos.
- Control y mantenimiento a los equipos.
- Implementación de nuevas aplicaciones para mejorar el sistema.
- Elaboración de un plan tecnológico y/o estratégico.

Asistente de sistemas:

- Dar soporte técnico a los usuarios.
- Realizar los inventarios de los equipos en conjunto con personal administrativo.
- Chequear las conexiones de datos con las diversas facultades de la UNP.
- Realizar correcciones de datos por errores de usuarios.
- Ciertas tareas de programación, así como también la configuración de redes.

Secretaría y Tramite Documentario:

- Planificar, organizar, dirigir y controlar los diversos documentos.
- Organizar y controlar reglamentariamente los diversos documentos y expedientes.
- Controlar el flujo y situación de los documentos dentro del CIT.
- Coordinar con todas las dependencias como facultades, sucursales de la UNP para el envió de archivos.

Asistencia Administrativa:

- Supervisa y ejecuta la realización del trabajo administrativo que, en razón de la competencia de la jefatura, esta decida asignarle.
- Redacta y envía la correspondencia a las unidades que lo requieran.
- Otras funciones encargadas por el Jefe de la Oficina Central.

Unidad de Soporte:

- Control de inventarios.
- Control del uso de las impresoras.
- Control del uso de los teléfonos.
- Soporte a los usuarios.

Unidad de Sistemas:

- Desarrollo de nuevas opciones en el Sistema.
- Mantenimiento de la Base de Datos.

- Control del consumo telefónico.
- Control de nuevas adquisiones tecnológicas por ejemplo protectores electrónicos.
- Correcciones en la base de datos como eliminaciones, cambio de fechas a movimientos, previa autorización del jefe de área.

Unidad de Telecomunicaciones:

- Mantenimiento de la red.
- Mantenimiento de la conexión a internet.

Practicantes:

- Dar soporte técnico a los usuarios
- Chequear las conexiones de datos con las diversas facultades de la UNP.
- Desarrollo de plataformas para el mejoramiento de los Sistemas de Información.
- Soporte de la red mediante el cableado por canaletas.

Como objetivos primordiales del Centro de Informática y Telecomunicaciones tenemos:

- Mejorar la plataforma tecnológica con el fin de optimizar los procesos operativos de la UNP.
- Mantener la información disponible y generar nueva información estadística en base a la necesidad de la organización
- Mediante el uso de la tecnología minimizar los costos operativos y de los servicios.
- Mantener el buen funcionamiento de los equipos de la red de computación y los programas

4.2.1 Arquitectura Informática

4.2.1.1 Sistema de Red de Computadoras en la UNP

La red de la UNP cuenta con Tecnologías de la Información (TI) en lo referente a: Sistemas de Comunicación, Sistemas de Información, Conectividad y Servicios Informáticos que se brinda de forma interna y externa a las diferentes Oficinas, Facultades, Dependencias. Se resume que la administración de Red está dividida en dos rubros:

a) Conectividad: Se encarga de la conexión alámbrica e inalámbrica de los equipos de comunicación.
b) Manejo de Servidores: Se encarga de alojar todos los servicios y sistemas de comunicación e información.

4.2.1.2 Sistema de Información en la UNP

El Sistema de Información, incluye la totalidad del Software de Aplicación, Software en Desarrollo, conjunto de Documentos Electrónicos, Bases de Datos e Información Histórica registrada en medios magnéticos e impresos en papeles, Documentos y Bibliografía.

El listado de Sistemas de Información en la Universidad Nacional de Piura, se detalla en el Anexo I.

4.2.2 Equipos disponibles

En toda la organización se cuentan con 374 equipos de cómputo distribuidos en todas las áreas y/o oficinas del CIT, los cuales están detallados a continuación:

N° de Piso	Nombre	Cantidad de PC
1	Informes 1	2
	Informes 2	2
	Auditorio 1	0
	Laboratorio 1	37
	Laboratorio 2	37
	Laboratorio 3	37
	Laboratorio 4	37
	Laboratorio 5	37
	Laboratorio 6	37
2	Instituto de Estudios Regionales	2
	Auditorio 2	0
	Aula 10	0
	Aula 11	0
	Aula 12	0
	Laboratorio 7	37
	Laboratorio 8	37
	Laboratorio 9	37
3	Secretaria	1
	Desarrollo Electrónico	4
	Sistemas Administrativos	3
	Desarrollo de Sistemas Académicos	4
	Desarrollo de Sistemas Administrativos	2
	Director General	2
4	Jefe Administrativo	2
	Almacén	0
	Archivos CIT	0
	Administrador de Telefonía	3
	Centro de Datos	6
5	Vicerrectorado de Investigación	2
	Sala de sesiones	1
	Vicerrector de investigación	2
	Oficina administrativa y secretaria	3
TOTAL		**374**

Tabla 2: Equipos de Cómputo
Fuente: Elaboración propia.

Adicionalmente en el CIT tenemos:

1er Piso:

- 1 Switch (Cisco Sistemas); Oficina.
- 3 Access Point Cisco AirNet 1200 series; lab 1,2,3

2do Piso:

- 2 SW Access 2960
- 1 Switch D-Link (Gigabit Poe)
- 2 Access Point; Lab 7,8

3er Piso:

- 1 Access Point(externo)
- 2 SW Acces 2960 Ethernet 10/100 de configuración fija (mesa de partes)

4to Piso:

- 1 Acces Point
- 1 Switch de 4 puertos

5to Piso:

- 1 Acces Point

La asignación de uso de las computadoras en cada área, se da para el jefe, asistente y el auxiliar o en todo caso practicante.

4.2.3 Sistema Operativo

El Sistema Operativo residente en el servidor del CIT es Windows 2003 Server, el resto de las computadoras posee diferentes versiones de Windows (XP, Vista, 7, 8) de acuerdo a las capacidades de cada equipo. A través del Servicio de "Active Directory" permite administrar a los usuarios sus derechos de acceso, ya sea por grupos o individualmente.

4.2.4 Software de Sistemas y Utilitarios

4.2.4.1 Lenguajes de Programación

En el área de sistemas del CIT se manejan los siguientes lenguajes de programación, así como gestores de base de datos:

- Java, C#, Php.
- SQL Server, para los procesos en la Base de Datos.

4.2.4.2 Sistemas de Información

La Institución tiene una relación de los Sistemas de información con los que cuenta, tanto los de desarrollo propio como los desarrollados por empresas externas (detallado en el Anexo I). Los Sistemas y Servicios críticos para la UNP, son los siguientes:

Listas de Sistemas

- **Sistema Integrado de Administración Financiera (SIAF):** Sistema de Información asociado a la ejecución del presupuesto anual de registro único de las operaciones de gastos e ingresos públicos, lo opera la Oficina Central de Ejecución Presupuestaria.

- **Sistema Integrado de Gestión Académica**: Sistema de información que permite el registro y control de los Procesos académicos, permite al alumno realizar consultas

académicas, consulta vía WEB. Lo operan las Oficinas Académicas y los órganos académicos-control.

- **Sistema de Tramite Documentario:** Sistema de información que permite el registro y seguimiento de los documentos. Lo operan todas las áreas funcionales.

- **Sistema de Gestión Administrativa – Ingresos:** Sistema de información que permite el registro y control de los ingresos, lo operan todas las áreas funcionales administrativas.

- **Sistema de Abastecimientos:** Sistema de información que permite el registro y control de las ordenes de trabajo, almacén, lo opera la Oficina de Abastecimiento.

- **Sistema de Control de Asistencia del personal:** Lo opera la oficina Central de Recursos Humanos.

- **Sistema de Banco de Preguntas para la elaboración de Exámenes de Admisión.**

- **Sistema de Gestión Docente.**

Listas de Servicios

- Sistema de comunicaciones.
- Servicio de Correo Corporativo.
- Servicios Web: Publicación de páginas Web, noticias de la UNP, Inscripción comedor universitario, Inscripción de cursos.
- Internet, Intranet.
- Servicios Proxy.
- VPN: Servicios de acceso privado a la red de la Institución desde cualquier lugar.

- Servicio de Monitoreo de la red: Monitorea los equipos de comunicación distribuidos en la red de la UNP.
- Servicios de telefonía principal: Teléfonos IP.
- Servicios de enseñanza de manera virtual.
- Servicio de Antivirus.

4.2.4.3 Software Básico y Utilitarios

La institución cuenta con el siguiente software básico y utilitario como apoyo para el desarrollo de sus actividades:

- Sistemas Operativos:
  - Windows XP, Vista, 7, 8.
  - Linux.
- Utilitarios:
  - Office 2010,2013.
  - Outlook Express
  - Acrobat Reader
  - Nero
  - Antivirus: Nod32, Kaspersky, Sophos.
  - Winrar

4.3 Identificación de los Riesgos

Para la identificación de los riesgos se aplicará la metodología Magerit mediante:

- Método de análisis de riesgos (MAR).
- Proceso de Gestión de Riesgos (PGR).

El desarrollo del análisis y gestión de riesgos del Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, se realiza mediante la metodología Magerit con el uso de la Herramienta PILAR 5.4.7 en su versión de prueba o de evaluación. Por lo cual se muestra el desarrollo de la metodología Magerit y a la par capturas de pantallas de su ejecución usando la herramienta Pilar.

Teniendo en cuenta que se realiza un análisis cualitativo porque el proyecto no se centra en aumentar ganancias y disminuir perdidas sino en plantear mejoras en la seguridad informática de los activos de información.

Datos del Proyecto

Código: DPSICIT -UNP

Nombre: DISEÑO DE UN PLAN DE SEGUIRDAD DE LA INFORMACION PARA EL CIT DE LA UNP, PERIODO 2015-2018.

Descripción: DISEÑO DE UN PLAN DE SEGUIRDAD DE LA INFORMACION PARA EL CIT DE LA UNP, PERIODO 2015-2018.

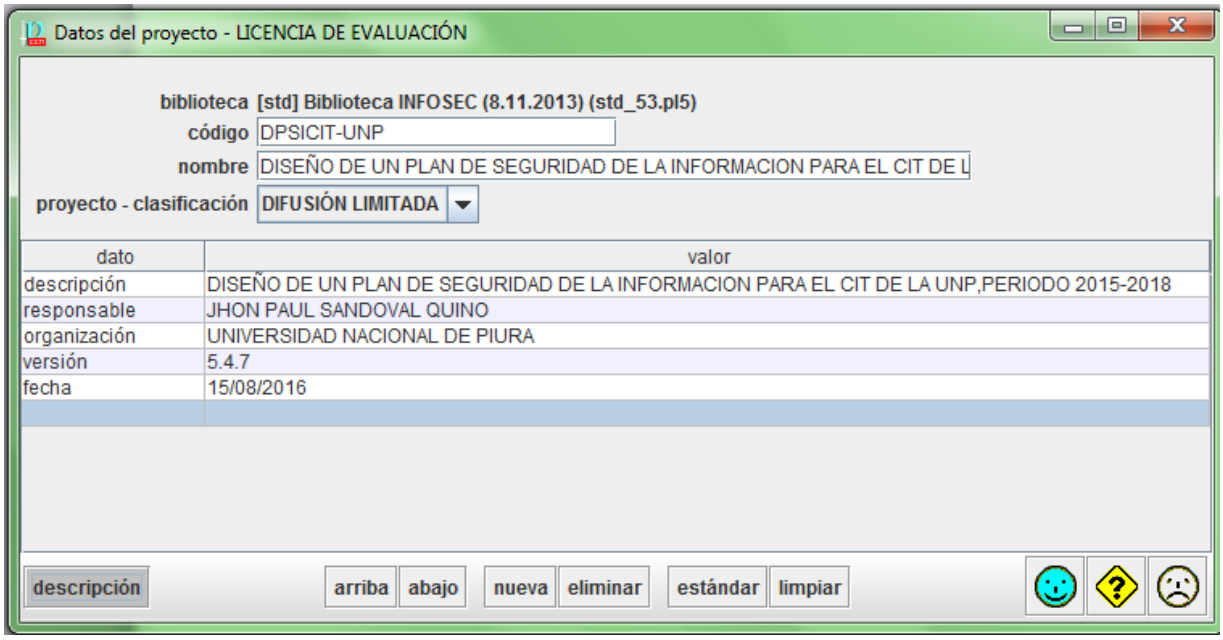


Gráfico 3: Datos del Proyecto DPSICIT-UNP – Pilar 5.4.7.

Fuente: Obtenido de la ejecución del Proyecto en la herramienta Pilar 5.4.7.

4.3.1 Método de Análisis de Riesgos (MAR)

Para la ejecución del proceso y la aplicación correcta de la metodología Magerit, el cual tiene como objetivos principales la identificación y estimación de los activos y de sus posibles amenazas, la recolección de la información fue obtenida a través de entrevistas, cuestionarios, aplicados al personal administrativo del CIT de la UNP.

Este proceso se desarrollará a través de un análisis cualitativo por lo ya expuesto, a continuación, una figura que muestra la pantalla de trabajo para el proceso de análisis de riesgos usando la herramienta Pilar 5.4.7.

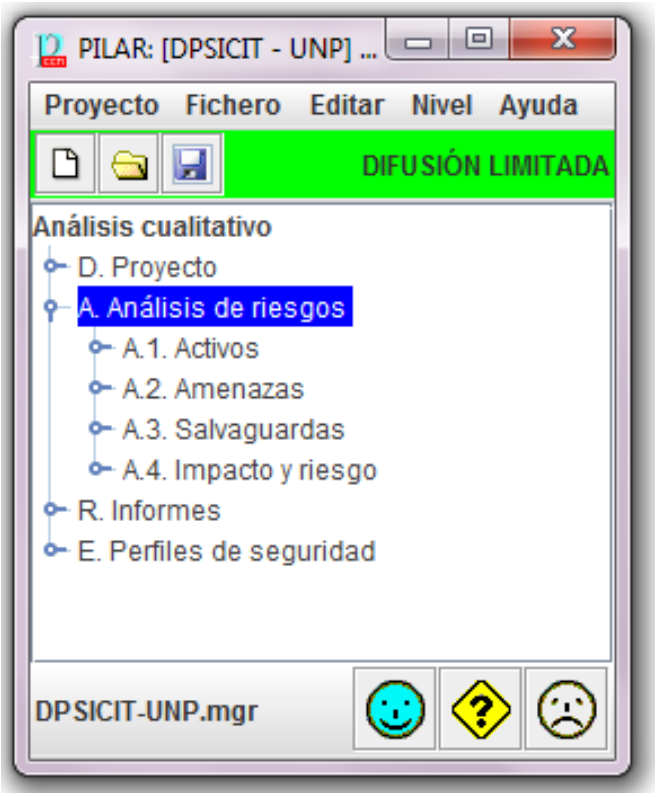


Gráfico 4: Análisis de Riesgos - DPSICIT-UNP

Fuente: Obtenido de la ejecución del Proyecto en la herramienta Pilar 5.4.7.

4.3.1.1 MAR 1: Caracterización de los Activos

El objetivo de las tareas englobadas en esta actividad es reconocer los activos que componen los procesos y definir las dependencias entre ellos. Así mismo realizar una valoración según la importancia que tenga cada activo para el caso de estudio.

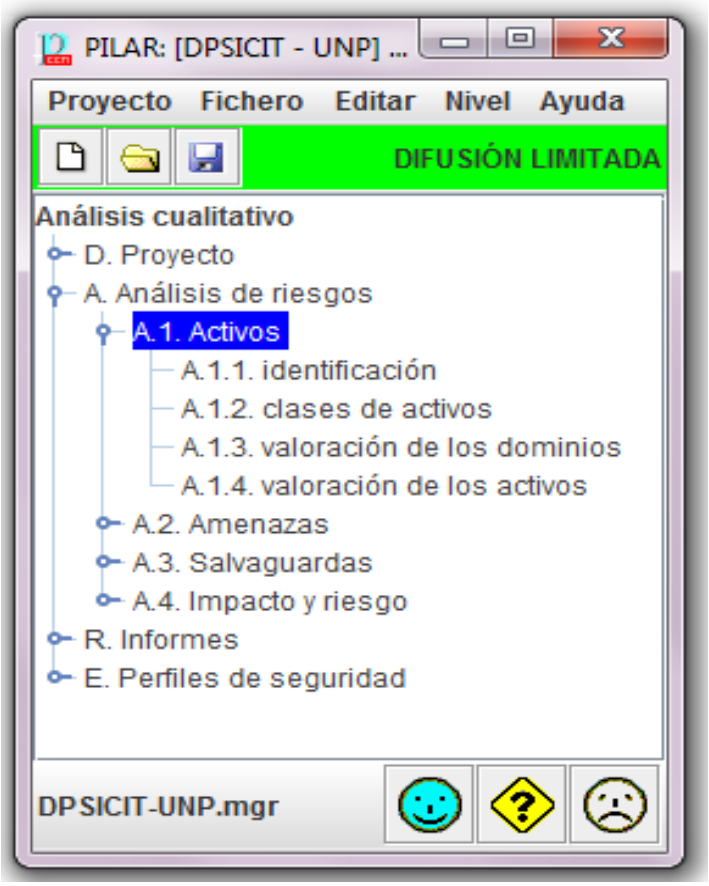


Gráfico 5: Caracterización de los activos - DPSICIT-UNP

Fuente: Obtenido de la ejecución del Proyecto en la herramienta Pilar 5.4.7.

4.3.1.1.1 Tarea MAR 1.1: Identificación de los Activos

Esta tarea es crítica por que una buena identificación permite realizar las siguientes tareas:

- Establecer las dependencias entre los activos.
- Permite valorar a los activos con precisión.

- Ayuda a identificar y valorar las amenazas.
- Escoge que salvaguardas serán necesarias para proteger el sistema.

El desarrollo a través de la herramienta Pilar, basada en la metodología Magerit, facilita la organización de los activos mediante el uso de capas generales, pero para el mejor entendimiento del objeto de estudio se realiza la estructuración mediante el tipo de activos, lo cual también se permite en la herramienta Pilar.

Los activos se agrupan en 8 capas según su tipo, como son servicios, software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y personal, a continuación, se realiza la identificación de los activos.

a) [S] Servicios

- [telf] Telefonía Ip.
- [inte] Internet.

b) [SW] Software (las aplicaciones informáticas)

- [Siaf]Sistema Integrado de Administración Financiera.
- [Siga]Sistema Integrado de Gestión Académico.
- [Sgad]Sistema de Gestión Administrativa.
- [Stdo]Sistema de Tramite documentario.
- [Saba]Sistema de Abastecimientos.
- [Scap]Sistema de Control de Asistencia del personal.
- [Sbpr]Sistema de Banco de Preguntas.
- [Sgdo]Sistema de Gestión Docente.

c) [HW] Hardware (los equipos informáticos)

- [Mimp]Medios de impresión
- [Cesc]Computadoras de escritorio
- [Spro]Servidor proxy

d) [COM]Redes de Comunicaciones

- [Rlan]Red LAN

- [Rwif]Red Wifi

e) [MEDIA]Soportes de Información

- [Disk]Discos.
- [Musb] Memoria USB.

f) [AUX]Equipamiento Auxiliar

- [Sain]Sistema de alimentación ininterrumpida

g) [L]Instalaciones

- [Edif]Edificio

h) [P]Personal

- [User]Usuarios Finales
  Serían los trabajadores administrativos

Al culminar la tarea se obtiene la lista de los 20 activos como se muestra en el siguiente Tabla.

ACTIVOS	
[S] Servicios	
	[telf.] Telefonía Ip.
	[inte] Internet
[SW] Software	
	[Siaf]Sistema Integrado de Administración Financiera.
	[Siga]Sistema Integrado de Gestión Académico.
	[Sgad]Sistema de Gestión Administrativa.
	[Stdo]Sistema de Tramite documentario.
	[Saba]Sistema de Abastecimientos.
	[Scap]Sistema de Control de Asistencia del personal.
	[Sbpr]Sistema de Banco de Preguntas.
	[Sgdo]Sistema de Gestión Docente.
[HW] Hardware	
	[Mimp]Medios de impresión
	[Cesc]Computadoras de escritorio
	[Spro]Servidor proxy
[COM]Redes de Comunicaciones	
	[Rlan]Red LAN
	[Rwif]Red Wifi
[MEDIA]Soportes de Información	
	[Disk]Discos
	[Musb]Memoria USB
[AUX]Equipamiento Auxiliar	
	[Sain]Sistema de alimentación ininterrumpida
[L]Instalaciones	
	[Edif]Edificio
[P]Personal	
	[User]Usuarios Finales

Tabla 3: Lista de activos- DPSICIT-UNP

Fuente: Obtenida de la Ejecución Del Proyecto en la Herramienta Pilar 5.4.7

4.3.1.1.2 Tara MAR 1.2: Dependencia entre los Activos

Una vez los activos son identificados hay que valorar las dependencias entre activos, es decir la medida en que un

activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

En el siguiente Tabla, teniendo en cuenta las dependencias para operar, funcionalidad y de almacenamiento de datos, se determina la siguiente matriz de dependencias entre activos (según el tipo de activos que corresponda):

	[S]	[SW]	[HW]	[COM]	[MEDIA]	[AUX]	[L]	[P]
[S]	-	**X**	**X**	**X**		**X**	**X**	**X**
[SW]		-						**X**
[HW]			-				**X**	**X**
[COM]				-			**X**	**X**
[MEDIA]					-			**X**
[AUX]						-	**X**	**X**
[L]							-	**X**
[P]								-

Tabla 4: Dependencia de activos según su tipo.

Fuente: Elaboración propia, basado en las actividades de la metodología Magerit.

Dónde:

[S]: Servicios.
[SW]: Software.
[HW]: Hardware.
[COM]: Redes de Comunicaciones.
[MEDIA]: Soportes de Información.
[AUX]: Equipamiento auxiliar.
[L]: Instalaciones.
[P]: Personal.

4.3.1.1.3 Tarea MAR 1.3: Valoración de los Activos

La tarea tiene como objetivos: Identificar en que dimensión es valioso el activo para la institución, la estimación de la valoración en cada dimensión.

ACTIVOS	D	I	C	A
[S] Servicios				
[telf.] Telefonía Ip.	A	B+	B+	A
[inte] Internet	A	B+	A	A
[COM]Redes de Comunicaciones				
[Rlan]Red LAN	B+	B+	B+	B+
[Rwif]Red Wifi	A	A	A	A
[SW] Software				
[Siaf]Sistema Integrado de Administración Financiera.	B+	B+	B+	B+
[Siga]Sistema Integrado de Gestión Académico.	B+	B+	B+	B+
[Sgad]Sistema de Gestión Administrativa.	B+	B+	B+	B+
[Stdo]Sistema de Tramite documentario.	B+	B+	B+	B+
[Saba]Sistema de Abastecimientos.	B+	B+	B+	B+
[Scap]Sistema de Control de Asistencia del personal.	B+	B+	B+	B+
[Sbpr]Sistema de Banco de Preguntas.	B+	B+	B+	B+
[Sgdo] Sistema de Gestión Docente	B+	B+	B+	B+
[HW] Hardware				
[Mimp]Medios de impresión	A	B+	A	A
[Cesc]Computadoras de escritorio	A	A	A	A
[Spro]Servidor proxy	A	A	A	A
[MEDIA]Soportes de Información				
[Disk]Discos	A	B+	A	A
[Musb)Memoria USB	A	A	A+	A
[AUX]Equipamiento Auxiliar				
[Sain]Sistema de alimentación ininterrumpida	A	A	A+	A
[L]Instalaciones				
[Edif]Edificio	A	A	A	A
[P]Personal				
[User]Usuarios Finales	A	A	A	A

Tabla 5: Valoración de Activos- DPSICIT-UNP.

Fuente: Obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.7 - Anexos (VIII al XI)

Se consideran dos datos importantes como dimensiones y criterios de valoración:

- **Dimensiones**

  - [D] Disponibilidad.
  - [I] Integridad de los datos.
  - [C] Confidencialidad de los datos.
  - [A] Autenticidad de los usuarios y de la información.

- **Criterios de la Valoración**

CRITERIOS		
Índice	**NIVEL**	**Índice**
A+	4	Pésimo
A	3	Regular
B+	2	Bueno
B	1	Excelente

Tabla 6: Escala detallada de los criterios de valoración**.**

ACTIVOS	[D]	[I]	[C]	[A]
[S] Servicios				
[telf.] Telefonía Ip.	A	A+	A+	A+
[inte] Internet	A	A+	A+	A+
[SW] Software				
[Siaf]Sistema Integrado de Administración Financiera.	A	A	A+	A+
[Siga]Sistema Integrado de Gestión Académico.	A	A	A+	A+
[Sgad]Sistema de Gestión Administrativa.	A	A	A+	A+
[Stdo]Sistema de Tramite documentario.	A	A	A+	A+
[Saba]Sistema de Abastecimientos.	A	A	A+	A+
[Scap]Sistema de Control de Asistencia del personal.	A	A	A+	A+
[Sbpr]Sistema de Banco de Preguntas.	A	A	A+	A+
[Sgdo] Sistema de Gestión Docente	A	A	A+	A+
[HW] Hardware				
[Mimp]Medios de impresión	A	A	A+	A+
[Cesc]Computadoras de escritorio	A	A	A+	A+
[Spro]Servidor proxy	A	A	A+	A+
[COM]Redes de Comunicaciones				
[Rlan]Red LAN	A	A	A+	A+
[Rwif]Red Wifi	A	A	A+	A+
[MEDIA]Soportes de información				
[Disk]Discos	A	A	A+	A+
[Musb)Memoria USB	A	A	A+	A+
[AUX]Equipamiento Auxiliar				
[Sain]Sistema de alimentación ininterrumpida	A	A	A+	A+
[L]Instalaciones				
[Edif]Edificio	A	A	A+	A+
[P]Personal				
[User]Usuarios Finales	A	A	A+	A+

Tabla 7: Valoración de Activos- Valor Acumulado- DPSICIT-UNP

Fuente: Obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.7

4.3.1.2 MAR 2: Caracterización de las Amenazas.

El objetivo en esta actividad es identificar las posibles amenazas que se pueden materializar sobre los activos y estimar la frecuencia de ocurrencia y degradación que causa.

En la siguiente figura se muestra la pantalla de trabajo para la caracterización de las amenazas. En el desarrollo usando la herramienta Pilar se presenta una opción de determinar la proporción de los factores para determinar las amenazas, para el estudio se toma la configuración pre determinada y se prosigue a la tarea siguiente.

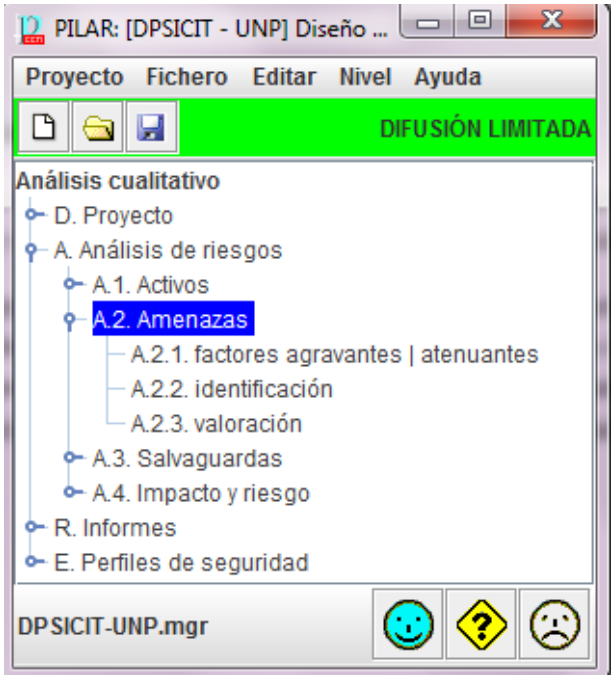


Gráfico 6: Pantalla de trabajo de caracterización de las amenazas.

Fuente: Obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.7

4.3.1.2.1 Tarea MAR 2.1: Identificación de las Amenazas.

El objetivo de la tarea es identificar las amenazas relevantes sobre cada activo en la herramienta Pilar estandarizada por Magerit, las amenazas están clasificadas en cuatro grupos:

- [N] Desastres Naturales
- [I] De origen industrial.
- [E] Errores y fallos no intencionados.
- [A] Ataque deliberados.

Se identifican las amenazas sobre cada activo.

Activos	Amenazas
Telefonía Ip.	[I.9] Interrupción de los servicios o suministros esenciales. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [A.5] Suplantación de la identidad. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.24] Denegación de servicio.
Internet.	[I.8] Fallo de servicios de comunicaciones. [I.9] Interrupción de los servicios o suministros esenciales. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [A.5] Suplantación de la identidad. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.24] Denegación de servicio.
Sistema Integrado de Administración Financiera.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software)

	[A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.22] Manipulación de programas.
Sistema Integrado de Gestión Académico.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software) [A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.22] Manipulación de programas.
Sistema de Gestión Administrativa.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software) [A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información

	[A.22] Manipulación de programas.
Sistema de Trámite Documentario.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software) [A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.22] Manipulación de programas.
Sistema de Abastecimientos.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software) [A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.22] Manipulación de programas.
Sistema de Control de Asistencia del Personal.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información.

	[E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software) [A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.22] Manipulación de programas.
Sistema de Banco de Preguntas.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software) [A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.22] Manipulación de programas.
Sistema de Gestión Docente.	[I.5]Avería de origen físico o lógico. [E.1] Errores de los usuarios. [E.2] Errores del administrador del sistema/de la seguridad [E.8] Difusión de software dañino. [E.15] Alteración de la información. [E.18] Destrucción de la información. [E.19] Fugas de información. [E.20]Vulnerabilidades de los programas (software). [E.21]Errores de mantenimiento / actualización de programas(software) [A.5] Suplantación de la identidad. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto.

	[A.8] Difusión de software dañino. [A.11] Acceso no autorizado. [A.15] Modificación de la información [A.18] Destrucción de la Información [A.19] Revelación de información [A.22] Manipulación de programas.
Medios de Impresión.	[N.1] Fuego. [N.2] Daños por agua [N.*] Desastres Naturales [I.1] Fuego [I.2]Daños por agua [I.*] Desastres Industriales. [I.3]Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico. [I.7] Condiciones Inadecuadas de Temperatura [I.11]Emanaciones electromagnéticas. [E.2]Errores del administrador del sistema/ de la seguridad [E.23]Errores de mantenimiento/actualización de equipos(hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Perdida de equipos. [A.7] Uso no previsto. [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo.
Computadoras de Escritorio.	[N.1] Fuego. [N.2] Daños por agua [N.*] Desastres Naturales [I.1] Fuego [I.2]Daños por agua [I.*] Desastres Industriales. [I.3]Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico. [I.7] Condiciones Inadecuadas de Temperatura [I.11]Emanaciones electromagnéticas. [E.2]Errores del administrador del sistema/ de la seguridad [E.23]Errores de mantenimiento/actualización de

	equipos(hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Perdida de equipos. [A.7] Uso no previsto. [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo.
Servidor Proxy.	[N.1] Fuego. [N.2] Daños por agua [N.*] Desastres Naturales [I.1] Fuego [I.2]Daños por agua [I.*] Desastres Industriales. [I.3]Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico. [I.7] Condiciones Inadecuadas de Temperatura [I.11]Emanaciones electromagnéticas. [E.2]Errores del administrador del sistema/ de la seguridad [E.23]Errores de mantenimiento/actualización de equipos(hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Perdida de equipos. [A.7] Uso no previsto. [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo.
Red Lan.	[I.8] Fallo de servicio de comunicaciones. [E.2] Errores del administrador del sistema/de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.6] Uso de privilegios de acceso. [A.7] Uso no previsto

	[A.9][re-]encanamiento de mensajes [A.10] Alteración de secuencia. [A.11]Acceso no autorizado [A.12] Análisis de trafico [A.14]Interceptación de información(escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de la información [A.24] Denegación de servicio.
Red Wifi.	[I.8] Fallo de servicio de comunicaciones. [E.2] Errores del administrador del sistema/de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.6] Uso de privilegios de acceso. [A.7] Uso no previsto [A.9][re-]encanamiento de mensajes [A.10] Alteración de secuencia. [A.11]Acceso no autorizado [A.12] Análisis de trafico [A.14]Interceptación de información(escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de la información [A.24] Denegación de servicio.
Discos.	[N.1] Fuego. [N.2] Daños por agua [N.*] Desastres Naturales [I.1] Fuego [I.2]Daños por agua [I.*] Desastres Industriales. [I.3]Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico. [I.7] Condiciones Inadecuadas de Temperatura [I.10] Degradación de los soportes de almacenamiento de la información [I.11]Emanaciones electromagnéticas. [E.1]Errores de los usuarios [E.15]Alteración de la información

	[E.18]Destrucción de la información [E.19] Fugas de información [E.23] Errores de mantenimiento/ actualización de equipos(hardware) [E.25] Pérdida de equipos. [A.7] Uso no previsto [A.11] Acceso no autorizado [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de la información [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo
Memoria USB.	[N.1] Fuego. [N.2] Daños por agua [N.*] Desastres Naturales [I.1] Fuego [I.2]Daños por agua [I.*] Desastres Industriales. [I.3]Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico. [I.7] Condiciones Inadecuadas de Temperatura [I.10] Degradación de los soportes de almacenamiento de la información [I.11]Emanaciones electromagnéticas. [E.1]Errores de los usuarios [E.15]Alteración de la información [E.18]Destrucción de la información [E.19] Fugas de información [E.23] Errores de mantenimiento/ actualización de equipos(hardware) [E.25] Pérdida de equipos. [A.7] Uso no previsto [A.11] Acceso no autorizado [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de la información [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo
Sistema de Alimentación Ininterrumpida.	[N.1] Fuego. [N.2] Daños por agua [N.*] Desastres Naturales [I.1] Fuego [I.2]Daños por agua [I.*] Desastres Industriales. [I.3]Contaminación medioambiental

	[E.23]Errores de mantenimiento/actualización de equipos(hardware) [A.7] Uso no previsto [A.23]Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo
Edificio.	[N.1] Fuego. [N.2] Daños por agua [N.*] Desastres Naturales [I.1] Fuego [I.2]Daños por agua [I.*] Desastres Industriales. [I.3]Contaminación medioambiental [I.4] Contaminación electromagnética [A.6]Abuso de privilegios de acceso [A.7] Uso no previsto [A.26] Ataque destructivo [A.27]Ocupación enemiga
Usuarios Finales.	[E.15]Alteración de la información [E.18]Destrucción de la información [E.19]Fugas de información [E.28]Indisponibilidad del personal [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.28]Indisponibilidad del personal [A.29]Extorsión [A.30]Ingeniería social(picaresca)

Tabla 8: Identificación de Amenazas a cada uno de los activos.
Fuente: Obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.7

4.3.1.2.2 Tarea MAR 2.1: Valoración de las Amenazas.

En la tarea Valoración de las Amenazas, se estima la frecuencia y la degradación de la materialización de las amenazas sobre cada activo identificado.

- Probabilidad de ocurrencia: representa la tasa anual de ocurrencia, de cada cuanto se materializa una amenaza.
- Porcentaje de degradación: significa el daño causado por un incidente.

La herramienta Pilar, tiene tablas de valores para la probabilidad de ocurrencia y el porcentaje de degradación, las cuales van a la par con las establecidas en la

metodología Magerit, para el estudio se usan las tablas propuestas por la herramienta Pilar.

Potencia	Probabilidad	Nivel	Facilidad	Frec.
XL extra grande	CS casi seguro	MA muy alto	F Fácil	100
L grande	MA muy alta	A alto	M medio	10
M medio	P posible	M medio	D difícil	1
S pequeño	PP poco probable	B bajo	MD muy difícil	0.1
XS muy pequeño	MR muy rara	MB muy bajo	ED extremadamente difícil	0.01

Tabla 9: Probabilidad.
Fuente: Obtenido del manual de usuario de Pilar.

Nivel		Porcentaje
T	Total	100%
MA	Muy Alta	90%
A	Alta	50%
M	Media	10%
B	Baja	1%

Tabla 10: Degradación
Fuente: Obtenido del manual de usuario de Pilar.

Posteriormente esta degradación se extiende debido a la dependencia entre activos, obteniendo el impacto y el riesgo, tanto acumulado como repercutido antes de aplicar las salvaguardas.

Si un activo A depende de otro B, el valor del impacto acumulado de A se acumula B en la proporción en la que depende. Por otro lado, el impacto repercutido indica que el daño en B en A en la proporción en la que A depende de B

Impacto= Valor x Degradación.

Tabla 11: Valoración de las amenazas- DPSICIT-UNP.

Activos	Amenazas	N	[D]	[I]	[C]	[A]
Telefonía Ip.	[I.9] Interrupción de los servicios o suministros esenciales.	M	A			
	[E.15] Alteración de la información.	M		M		
	[E.18] Destrucción de la información	M	M			
	[E.19] Fugas de información	M			M	
	[A.5] Suplantación de la identidad.	B		T	T	T
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la información.	M	A			
	[A.19] Revelación de información	M			A	
	[A.24] Denegación de servicio.	M	A			
Internet.	[I.8] Fallo de servicios de comunicaciones.	M				
	[I.9] Interrupción de los servicios o suministros esenciales.	0	A			
	[E.15] Alteración de la información.	M		M		
	[E.18] Destrucción de la información	M	M			
	[E.19] Fugas de información	M			M	
	[A.5] Suplantación de la identidad.	B		T	T	T
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la información.	M	A			
	[A.19] Revelación de información	M			A	
	[A.24] Denegación de servicio.	M	A			
Sistema Integrado de Administración Financiera.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	

	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la Información	M	A			
	[A.19] Revelación de información	M			A	
	[A.22] Manipulación de programas.	M	A	T	T	
Sistema Integrado de Gestión Académico.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la Información	M	A			
	[A.19] Revelación de información	M			A	
	[A.22] Manipulación de programas.	M	A	T	T	
Sistema de Gestión Administrativa.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	
	[A.15] Modificación de la información	M		A		

	[A.18] Destrucción de la Información	M	A			
	[A.19] Revelación de información	M			A	
	[A.22] Manipulación de programas.	M	A	T	T	
Sistema de Trámite Documentario.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la Información	M	A			
	[A.19] Revelación de información	M			A	
	[A.22] Manipulación de programas.	M	A	T	T	
Sistema de Abastecimientos.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la Información	M	A			

	[A.19] Revelación de información	M			A	
	[A.22] Manipulación de programas.	M	A	T	T	
Sistema de Control de Asistencia del Personal.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la Información	M	A			
	[A.19] Revelación de información	M			A	
	[A.22] Manipulación de programas.	M	A	T	T	
Sistema de Banco de Preguntas.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la Información	M	A			
	[A.19] Revelación de información	M			A	

	[A.22] Manipulación de programas.	M	A	T	T	
Sistema de Gestión Docente.	[I.5] Avería de origen físico o lógico.	M	A			
	[E.1] Errores de los usuarios.	M	B	M	M	
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.8] Difusión de software dañino.	M	M	M	M	
	[E.15] Alteración de la información.	M		B		
	[E.18] Destrucción de la información.	M	A			
	[E.19] Fugas de información.	M			M	
	[E.20]Vulnerabilidades de los programas (software).	M	B	M	M	
	[E.21]Errores de mantenimiento / actualización de programas(software)	A	B	B		
	[A.5] Suplantación de la identidad.	M		A	A	T
	[A.6] Abuso de privilegios de acceso.	M	B	M	M	
	[A.7] Uso no previsto.	M	B	M	M	
	[A.8] Difusión de software dañino.	M	T	T	T	
	[A.11] Acceso no autorizado.	M		M	A	
	[A.15] Modificación de la información	M		A		
	[A.18] Destrucción de la Información	M	A			
	[A.19] Revelación de información	M			A	
	[A.22] Manipulación de programas.	M	A	T	T	
Medios de Impresión.	[N.1] Fuego.	B	T			
	[N.2] Daños por agua	B	A			
	[N.*] Desastres Naturales	B	T			
	[I.1] Fuego	M	T			
	[I.2]Daños por agua	M	A			
	[I.*] Desastres Industriales.	M	T			
	[I.3]Contaminación medioambiental	B	A			
	[I.4] Contaminación electromagnética	M	M			
	[I.5] Avería de origen físico o lógico	M	A			
	[I.6] Corte de suministro eléctrico.	M	T			
	[I.7] Condiciones Inadecuadas de Temperatura	M	T			
	[I.11]Emanaciones electromagnéticas.	M			B	
	[E.2]Errores del administrador del sistema/ de la seguridad	M	M	M	M	
	[E.23]Errores de mantenimiento/actualización de equipos(hardware)	M	M			
	[E.24] Caída del sistema por agotamiento de recursos	A	A			
	[E.25] Perdida de equipos.	M	T		A	

	[A.7] Uso no previsto	M	M	M	M	
	[A.11] Acceso no autorizado	M	M	B	A	
	[A.23] Manipulación del hardware	M	A	M	A	
	[A.24] Denegación de servicio	M	T			
	[A.25] Robo de equipos	M	T		A	
	[A.26] Ataque destructivo.	M	T			
Computadoras de Escritorio.	[N.1] Fuego.	B	T			
	[N.2] Daños por agua	B	A			
	[N.*] Desastres Naturales	B	T			
	[I.1] Fuego	M	T			
	[I.2]Daños por agua	M	A			
	[I.*] Desastres Industriales.	M	T			
	[I.3]Contaminación medioambiental	B	A			
	[I.4] Contaminación electromagnética	M	M			
	[I.5] Avería de origen físico o lógico	M	A			
	[I.6] Corte de suministro eléctrico.	M	T			
	[I.7] Condiciones Inadecuadas de Temperatura	M	T			
	[I.11]Emanaciones electromagnéticas.	M			B	
	[E.2]Errores del administrador del sistema/ de la seguridad	M	M	M	M	
	[E.23]Errores de mantenimiento/actualización de equipos(hardware)	M	M			
	[E.24] Caída del sistema por agotamiento de recursos	A	A			
	[E.25] Perdida de equipos.	A	M		M	
	[A.7] Uso no previsto	M	M	M	M	
	[A.11] Acceso no autorizado	M	M	B	A	
	[A.23] Manipulación del hardware	M	A	M	A	
	[A.24] Denegación de servicio	M	T			
	[A.25] Robo de equipos	A	M		M	
	[A.26] Ataque destructivo.	M	T			
Servidor Proxy.	[N.1] Fuego.	B	T			
	[N.2] Daños por agua	B	A			
	[N.*] Desastres Naturales	B	T			
	[I.1] Fuego	M	T			
	[I.2]Daños por agua	M	A			
	[I.*] Desastres Industriales.	M	T			
	[I.3]Contaminación medioambiental	B	A			
	[I.4] Contaminación electromagnética	M	M			
	[I.5] Avería de origen físico o lógico	M	A			
	[I.6] Corte de suministro eléctrico.	M	T			

	[I.7] Condiciones Inadecuadas de Temperatura	M	T			
	[I.11]Emanaciones electromagnéticas.	M			B	
	[E.2]Errores del administrador del sistema/ de la seguridad	M	M	M	M	
	[E.23]Errores de mantenimiento/actualización de equipos(hardware)	M	M			
	[E.24] Caída del sistema por agotamiento de recursos	A	A			
	[E.25] Perdida de equipos.	B	T		T	
	[A.7] Uso no previsto	M	B	M	M	
	[A.11] Acceso no autorizado	M	M	B	A	
	[A.23] Manipulación del hardware	M	A	M	A	
	[A.24] Denegación de servicio	M	T			
	[A.25] Robo de equipos	B	T		T	
	[A.26] Ataque destructivo.	M	T			
Red Lan.	[I.8] Fallo de servicio de comunicaciones.	M	A			
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.9] Errores de [re-]encaminamiento	M			M	
	[E.10] Errores de secuencia	M		M		
	[E.15] Alteración de la información	M		B		
	[E.19] Fugas de información	M			M	
	[E.24] Caída del sistema por agotamiento de recursos	M	A			
	[A.5] Suplantación de la identidad	M		M	A	T
	[A.6] Uso de privilegios de acceso	M		M	A	T
	[A.7] Uso no previsto	M	M	M	M	
	[A.9][re-]encanamiento de mensajes	M			M	
	[A.10] Alteración de secuencia.	M		M		
	[A.11]Acceso no autorizado	M		M	A	T
	[A.12] Análisis de trafico	M			B	
	[A.14]Interceptación de información(escucha)	M			B	
	[A.15] Modificación de la información	M		M		
	[A.18] Destrucción de la información	M	A			
	[A.19] Revelación de la información	M			A	
	[A.24] Denegación de servicio.	A	A			
Red Wifi.	[I.8] Fallo de servicio de comunicaciones.	M	A			
	[E.2] Errores del administrador del sistema/de la seguridad	M	M	M	M	
	[E.9] Errores de [re-]encaminamiento	M			M	

	[E.10] Errores de secuencia	M		M		
	[E.15] Alteración de la información	M		B		
	[E.19] Fugas de información	M			M	
	[E.24] Caída del sistema por agotamiento de recursos	M	A			
	[A.5] Suplantación de la identidad	M		M	A	T
	[A.6] Uso de privilegios de acceso	M		M	A	T
	[A.7] Uso no previsto	M	M	M	M	
	[A.9][re-]encanamiento de mensajes	M			M	
	[A.10] Alteración de secuencia.	M		M		
	[A.11]Acceso no autorizado	M		M	A	T
	[A.12] Análisis de trafico	M			B	
	[A.14]Interceptación de información(escucha)	M			M	
	[A.15] Modificación de la información	M		M		
	[A.18] Destrucción de la información	M	A			
	[A.19] Revelación de la información	M			A	
	[A.24] Denegación de servicio.	A	A			
Discos.	[N.1] Fuego.	B	T			
	[N.2] Daños por agua	B	A			
	[N.*] Desastres Naturales	B	T			
	[I.1] Fuego	M	T			
	[I.2]Daños por agua	M	A			
	[I.*] Desastres Industriales.	M	T			
	[I.3]Contaminación medioambiental	M	A			
	[I.4] Contaminación electromagnética	M	M			
	[I.5] Avería de origen físico o lógico	M	A			
	[I.6] Corte de suministro eléctrico.	M	T			
	[I.7] Condiciones Inadecuadas de Temperatura	M	T			
	[I.10] Degradación de los soportes de almacenamiento de la información	M	T			
	[I.11]Emanaciones electromagnéticas.	M			B	
	[E.1]Errores de los usuarios	M	B	M	M	
	[E.15]Alteración de la información	M		B		
	[E.18]Destrucción de la información	M	T			
	[E.19] Fugas de información	M			M	
	[E.23] Errores de mantenimiento/ actualización de equipos(hardware)	M	T			
	[E.25] Pérdida de equipos.	M	M		A	
	[A.7] Uso no previsto	M	B		B	
	[A.11] Acceso no autorizado	M		B	A	
	[A.15] Modificación de la información	A		T		

	[A.18] Destrucción de la información	M	T			
	[A.19] Revelación de la información	M			M	
	[A.23] Manipulación del hardware	B	A		A	
	[A.25] Robo de equipos	M	M		T	
	[A.26] Ataque destructivo	M	M			
Memoria USB.	[N.1] Fuego.	B	T			
	[N.2] Daños por agua	B	A			
	[N.*] Desastres Naturales	B	T			
	[I.1] Fuego	M	T			
	[I.2]Daños por agua	M	A			
	[I.*] Desastres Industriales.	M	T			
	[I.3]Contaminación medioambiental	M	A			
	[I.4] Contaminación electromagnética	M	M			
	[I.5] Avería de origen físico o lógico	M	A			
	[I.6] Corte de suministro eléctrico.	M	T			
	[I.7] Condiciones Inadecuadas de Temperatura	M	T			
	[I.10] Degradación de los soportes de almacenamiento de la información	M	T			
	[I.11]Emanaciones electromagnéticas.	M			B	
	[E.1]Errores de los usuarios	M	B	M	M	
	[E.15]Alteración de la información	M		B		
	[E.18]Destrucción de la información	M	T			
	[E.19] Fugas de información	M			M	
	[E.23] Errores de mantenimiento/ actualización de equipos(hardware)	M	T			
	[E.25] Pérdida de equipos.	M	M		A	
	[A.7] Uso no previsto	M	B		B	
	[A.11] Acceso no autorizado	M		B	A	
	[A.15] Modificación de la información	M		T		
	[A.18] Destrucción de la información	M	T			
	[A.19] Revelación de la información	M			M	
	[A.23] Manipulación del hardware	B	A		A	
	[A.25] Robo de equipos	M	M		T	
	[A.26] Ataque destructivo	M	M			
Sistema de Alimentación Ininterrumpida.	[N.1] Fuego.	B	B			
	[N.2] Daños por agua	B	B			
	[N.*] Desastres Naturales	B	B			
	[I.1] Fuego	M	B			
	[I.2]Daños por agua	M	B			
	[I.*] Desastres Industriales.	M	B			
	[I.3]Contaminación medioambiental	B	B			

	[E.23]Errores de mantenimiento/actualización de equipos(hardware)	M	B			
	[A.7] Uso no previsto	M	B	0	0	
	[A.23]Manipulación del hardware	M	B		0	
	[A.25] Robo de equipos	M	B			
	[A.26] Ataque destructivo	M	B			
Edificio.	[N.1] Fuego.	M	T			
	[N.2] Daños por agua	M	T			
	[N.*] Desastres Naturales	M	T			
	[I.1] Fuego	M	T			
	[I.2]Daños por agua	M	T			
	[I.*] Desastres Industriales.	M	T			
	[I.3]Contaminación medioambiental	M	M			
	[I.4] Contaminación electromagnética	B	M			
	[A.6]Abuso de privilegios de acceso	M	M	M	A	
	[A.7] Uso no previsto	M	M	M	A	
	[A.26] Ataque destructivo	B	T			
	[A.27]Ocupación enemiga	M	T		A	
Usuarios Finales.	[E.15]Alteración de la información	M		M		
	[E.18]Destrucción de la información	M	B			
	[E.19]Fugas de información	M			M	
	[E.28]Indisponibilidad del personal	M	M			
	[A.15]Modificación de la información	M		A		
	[A.18]Destrucción de la información	M	M			
	[A.19]Revelación de información	A			A	
	[A.28]Indisponibilidad del personal	M	M			
	[A.29]Extorsión	M	B	T	T	
	[A.30]Ingeniería social(picaresca)	M	B	T	T	

Fuente: Proyecto Pilar DPSICIT-UNP.

4.3.1.3 MAR 3: Caracterización de las Salvaguardas.

En esta actividad se identifican las salvaguardas efectivas para la organización junto con la eficacia que tiene cada una de ellas para mitigar el riesgo. En el desarrollo de la metodología se definen varias etapas, para el estudio se a determinado las siguientes:

- Primera etapa llamada POTENCIAL potencial), desde el inicio de la creación del proyecto hasta la caracterización de amenazas.

- Segunda etapa llamada SITUACION ACTUAL (actual), toma los resultados de la primera etapa incluyendo la influencia de las salvaguardas implantadas hasta el momento.
- Tercera etapa OBJETIVO (objetivo), recoge los datos de las dos etapas anteriores, pero también hace referencia a los posibles resultados tras el plan de mitigación. En esta etapa se desarrolla el Proceso de Gestión de Riesgos.

En la herramienta Pilar para el desarrollo de la actividad se toma en cuenta los siguientes Tablas:

Abreviaturas	Aspecto (que trata la salvaguarda)
G	para Gestión
T	para Técnico
F	para Seguridad Física
P	para Gestión del Personal

Tabla 12: Aspecto de las salvaguardas
Fuente: Obtenida del manual de usuarios de Pilar.

Abreviatura	Tipo de protección de salvaguardas
PR	Prevención
DR	Disuasión
EL	Eliminación
IM	Minimización del impacto
CR	Corrección
RC	Recuperación
AD	Administrativa
AW	Concienciación
DC	Detención
MN	Monitorización

Tabla 13: Tipo de protección de las salvaguardas.
Fuente: Obtenida del manual de usuarios de Pilar.

PILAR	Valoración		
		Máximo peso	Critica
		Peso alto	Muy importante
		Peso normal	Importante
		Peso bajo	Interesante

Tabla 14: Peso relativo de las salvaguardas.
Fuente: Obtenida del manual de usuarios de Pilar.

4.3.1.3.1 Tarea MAR 3.1: Identificación de las Salvaguardas Existentes

Su objetivo principal es identificar las salvaguardas convenientes para proteger el sistema, en esta tarea contaremos con la ayuda de la herramienta PILAR 5.4.7 que nos ayuda a la elección de salvaguardas de cada activo para contrarrestar las amenazas identificadas.

- **Protecciones Generales**

  A continuación, las salvaguardas que fueran escogidas:

  - Se requiere autorización previa: pertenece al grupo de restricción de acceso a la información que a su vez pertenece al control de acceso lógico; se escogió esta salvaguarda ya que cualquier persona puede acceder a los activos inclusive los más importantes, esta puede ser aplicada a estas clases de activos: Datos/Información, Servicios, Aplicaciones (software), equipamiento informático (hardware), redes de comunicaciones y soportes de información.

  Protege a las dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad.

- **Protección de los Servicios**

  La salvaguarda plantea el aseguramiento de la disponibilidad, así como la gestión de cambios y aplicación de perfiles de seguridad buscando brindar un servicio con un alto grado de calidad.

- **Protección de las aplicaciones informáticas (SW)**

  Se seleccionó las siguientes salvaguardas ya que la organización no posee estas normas de seguridad como son:

  - Se dispone de normativa sobre el uso autorizado de las aplicaciones.

- Se dispone de normativa relativa al cumplimiento de los derechos.
- Se controla la instalación de software autorizado y productos con licencia.
- Se dispone de procedimientos para realizar copias de seguridad.

Se debería tratar de cumplir con lo siguiente:

- Seguridad de los ficheros de datos de la aplicación.
- Se protegen los ficheros de configuración.
- Seguridad de los mecanismos de comunicación entre procesos.

Asegurar las dimensiones de seguridad como confidencialidad e integridad

- Se debe llevar un control de versión de toda la actualización de software, esto ayuda a saber que cualquier software que posee la organización esté libre de errores y hacer frente a amenazas como son: vulnerabilidades de los programas (software) y errores de mantenimiento/actualización de programas (software).

- **Protección de los equipos informáticos (HW)**

A continuación, las salvaguardas adecuadas para la protección de los equipos informáticos:

- Se dispone de normativa sobre el uso correcto de los equipos.
- Se dispone de procedimientos de uso de equipamiento.
- Se aplican perfiles de seguridad: si se implementa esta salvaguarda en la organización, minimiza amenazas como son: errores del administrador del sistema/ de la seguridad, uso no previsto y acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad.

Además, se debe de tener en cuenta estas salvaguardas al momento de utilizar los equipos como son:

- Protección física de los equipos: son mecanismos que la organización no ha tomado en cuenta para proteger la información principalmente sobre un activo que es el servidor de datos

    - Para evitar accesos innecesarios
    - Para evitar acceso no autorizado
- Seguridad del equipamiento de oficina.

Después de evaluar las salvaguardas antes mencionadas, se debe implantar las siguientes salvaguardas:

- Se evalúa el impacto en la confidencialidad de los datos
- Se evalúa el impacto en la integridad de los datos.

- **Protección de las comunicaciones**

Se han escogido las siguientes salvaguardas para minimizar riesgos:

- Se debe de aplicar perfiles de seguridad: para garantizar la comunicación en la organización y para hacer frente a amenazas como: Errores de [re]- encadenamiento de mensajes, errores de secuencia, alteración de la información, uso no previsto, [re]- encaminamiento de mensajes, alteración de secuencia y acceso no autorizado, además proteger las dimensiones de seguridad: integridad, confidencialidad y autenticidad.
- La organización no posee de normativa de uso de los servicios de red.
- Así mismo no dispone de un control de filtrado
- No dispone de mecanismos como son:
    - Comprobación de origen y destino
    - Mecanismos de control
- No tiene ninguna seguridad de los servicios de red.

Para garantizar las comunicaciones cuando están utilizando el internet es necesario emplear las siguientes salvaguardas:

- Herramienta de control de contenidos con filtros actualizados.
- Controlar la configuración de los navegadores.
- Registrar la descarga.
- Instalar herramientas anti spyware.
- Deshabilitar los "cookies" en los navegadores.
- Registrar la navegación web.
- Disponer de normativa sobre el uso de los servicios Internet.
- Herramienta de monitorización de tráfico.
- Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios.

- **Protección de los soportes de información**

Se ha escogido la salvaguarda más apropiado el cual es:

- Disponer de normativa de relativa a la protección criptográfica de los contenidos.

- **Elementos auxiliares**

Se asegura la disponibilidad:

- Siguiendo las recomendaciones del fabricante o proveedor.
- Continuidad de operaciones: para asegurar la disponibilidad de los equipos auxiliares además para contrarrestar la amenaza de contaminación medioambiental.
- Climatización: la adecuada climatización de cada equipo ayuda a enfrentar la amenaza que tiene la mayoría de estos componentes que es, condiciones inadecuadas de temperatura o humedad.

- **Protección de las instalaciones**

  - Se dispone de normativa de seguridad para la seguridad de las instalaciones.
  - Se dispone de áreas específicas para equipos informáticos, para protegerlos de la ocupación enemiga.
  - Además de la protección del perímetro y reforzar la vigilancia en las instalaciones de la organización.
  - Protección frente a explosivos.

- **Gestión del personal**

  - Se dispone de normativa relativa a la gestión de personal (materia de seguridad).
  - Se dispone de procedimientos para la gestión de personal (materia de seguridad).
  - Creación de normas del personal: propio y subcontratado.
  - Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo.
  - Se establecen normas para la contratación de personal, para garantizar la confidencialidad de los datos, frente a ataques cómo Extorsión y Ataque desde el interior.
  - Procedimientos relevantes de seguridad: emergencias, incidencias.

- **Adquisición / Desarrollo**

  La salvaguarda plantea la compra o el desarrollo de aplicaciones, equipos informáticos, de comunicaciones, de soporte de información o comunicaciones que aporten a la mejora del servicio. Hace frente a amenazas como: errores de usuarios, errores del administrador del sistema / de la seguridad, difusión de software dañino, alteración de la información, fugas de información, vulnerabilidad de los sistemas, errores de mantenimiento / actualización de programas, perdida de equipos, abuso de privilegios de acceso y uso no previsto.

[base] Base Seguridad			
Aspecto	Tdp	Salvaguardas	Recom
G	PR	[H] Protecciones Generales	7
G	PR	[S] Protecciones de los Servicios	5
G	PR	[SW] Protección de las aplicaciones informáticas	6
G	PR	[HW] Protección de los equipos informáticos	5
G	PR	[COM]Protección de las comunicaciones	8
G	PR	[MP] Protección de los soportes de información	6
G	PR	[AUX] Elementos auxiliares	6
F	PR	[L] Protección de las instalaciones	6
P	PR	[PS] Gestión del Personal	6
G	AD	[New] Adquisición/desarrollo	5

Tabla 15: Lista de salvaguardas existentes y valoración de Pilar.
Fuente: Proyecto DPSICIT-UNP – Pilar 5.4.7.

4.3.1.3.2 Tarea MAR 3.2: Valoración de las Salvaguardas

El objetivo de esta tarea es determinar la eficacia de las salvaguardas pertinentes.

Eficacia	Nivel	Madurez	Estado
0%	L0	inexistente	inexistente
10%	L1	inicial/ad hoc	iniciado
50%	L2	reproducible, pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Tabla 16: Niveles de madurez.
Fuente: Herramienta Pilar 5.4.7.

4.3.1.4 MAR 4: Estimación del Estado de Riesgo.

En esta tarea se combinan los descubrimientos de las tareas anteriores para derivar estimaciones del estado de riesgo de la Organización.

Esta actividad consta de dos tareas:

- Estimación del impacto.
- Estimación del riesgo.

El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

4.3.1.4.1 Tarea MAR 4.1: Estimación del impacto

En esta tarea se estima el impacto al que están expuestos los activos:

- El impacto potencial, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- El impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

CRITERIOS			
10	Nivel 10	10	
9	Nivel 9	9	
A+	Nivel alto +	8	
A	nivel alto	7	
A-	nivel alto -	6	
M+	nivel medio +	5	
M	nivel medio	4	
M-	nivel medio -	3	
B+	nivel bajo +	2	
B	nivel bajo	1	
0	sin valor apreciable	0	

Tabla 17: Estimación del impacto.

Fuente: Manual de usuario de Pilar.

4.3.1.4.1.1 Impacto Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materializacion de una amenaza.Conociendo el valor de los activos(en varias dimensiones) y la degradación que causan las amenazas, es directo el impacto que estas tendrian sobre el sistema.

ACTIVOS	[D]	[I]	[C]	[A]
[S] Servicios				
[telf.] Telefonía Ip.	2	4	4	4
[inte] Internet	3	4	4	4
[SW] Software				
[Siaf]Sistema Integrado de Administración Financiera.	3	3	4	4
[Siga]Sistema Integrado de Gestión Académico.	3	3	4	4
[Sgad]Sistema de Gestión Administrativa.	3	3	4	4
[Stdo]Sistema de Tramite documentario.	3	3	4	4
[Saba]Sistema de Abastecimientos.	3	3	4	4
[Scap]Sistema de Control de Asistencia del personal.	3	3	4	4
[Sbpr]Sistema de Banco de Preguntas.	3	3	4	4
[Sgdo] Sistema de Gestión Docente	3	3	4	4
[HW] Hardware				
[Mimp]Medios de impresión	3	1	3	
[Cesc]Computadoras de escritorio	3	1	3	
[Spro]Servidor proxy	3	1	4	
[COM]Redes de Comunicaciones				
[Rlan]Red LAN	2	1	3	4
[Rwif]Red Wifi	2	1	3	4
[MEDIA]Soportes de información				
[Disk]Discos	3	4	4	
[Musb)Memoria USB	3	4	4	
[AUX]Equipamiento Auxiliar				
[Sain]Sistema de alimentación ininterrumpida	1			
[L]Instalaciones				
[Edif]Edificio	3	1	3	
[P]Personal				
[User]Usuarios Finales	1	3	4	

Tabla 18: Impacto Potencial.
Fuente: Proyecto DPSICIT-UNP – Pilar 5.4.7.

4.3.1.4.1.2 Impacto Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

ACTIVOS	[D]	[I]	[C]	[A]
[S] Servicios				
[telf] Telefonía Ip.	2	2	2	3
[inte] Internet	3	2	3	3
[SW] Software				
[Siaf]Sistema Integrado de Administración Financiera.	2	2	2	2
[Siga]Sistema Integrado de Gestión Académico.	2	2	2	2
[Sgad]Sistema de Gestión Administrativa.	2	2	2	2
[Stdo]Sistema de Tramite documentario.	2	2	2	2
[Saba]Sistema de Abastecimientos.	2	2	2	2
[Scap]Sistema de Control de Asistencia del personal.	2	2	2	2
[Sbpr]Sistema de Banco de Preguntas.	2	2	2	2
[Sgdo] Sistema de Gestión Docente	2	2	2	2
[HW] Hardware				
[Mimp]Medios de impresión	3	2	3	3
[Cesc]Computadoras de escritorio	3	2	3	3
[Spro]Servidor proxy	3	3	4	3
[COM]Redes de Comunicaciones				
[Rlan]Red LAN	3	2	2	2
[Rwif]Red Wifi	2	3	3	3
[MEDIA]Soportes de información				
[Disk]Discos	3	1	3	3
[Musb)Memoria USB	3	3	3	4
[AUX]Equipamiento Auxiliar				
[Sain]Sistema de alimentación ininterrumpida	3	3	3	4
[L]Instalaciones				
[Edif]Edificio	3	3	3	3
[P]Personal				
[User]Usuarios Finales	3	3	3	3

Tabla 19: Impacto Residual
Fuente: Proyecto DPSICIT-UNP – Pilar 5.4.7.

4.3.1.4.2 Tarea MAR 4.2: Estimación del Riesgo.

En esta tarea se estima el riesgo al que están sometidos los activos del sistema: el riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.

El riesgo residual, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

CRITERIOS			
9	Nivel 9	9	
A+	Nivel alto +	8	
A	nivel alto	7	
A-	nivel alto -	6	
M+	nivel medio +	5	
M	nivel medio	4	
M-	nivel medio -	3	
B+	nivel bajo +	2	
B+	nivel bajo	1	
0	sin valor apreciable	0	

Tabla 20: Criterios de Estimación del Riesgo
Fuente: Proyecto DPSICIT-UNP – Pilar 5.4.7.

4.3.1.4.2.1 Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener la probabilidad de ocurrencia.

ACTIVOS	[D]	[I]	[C]	[A]
[S] Servicios				
[telf.] Telefonía Ip.	{2,2}	{2,8}	{2,8}	{2,7}
[inte] Internet	{2,7}	{2,8}	{2,8}	{2,7}
[SW] Software				
[Siaf]Sistema Integrado de Administración Financiera.	{2,7}	{2,7}	{3,3}	{3,3}
[Siga]Sistema Integrado de Gestión Académico.	{2,7}	{2,7}	{3,3}	{3,3}
[Sgad]Sistema de Gestión Administrativa.	{2,7}	{2,7}	{3,3}	{3,3}
[Stdo]Sistema de Tramite documentario.	{2,7}	{2,7}	{3,3}	{3,3}
[Saba]Sistema de Abastecimientos.	{2,7}	{2,7}	{3,3}	{3,3}
[Scap]Sistema de Control de Asistencia del personal.	{2,7}	{2,7}	{3,3}	{3,3}
[Sbpr]Sistema de Banco de Preguntas.	{2,7}	{2,7}	{3,3}	{3,3}
[Sgdo] Sistema de Gestión Docente	{2,7}	{2,7}	{3,3}	{3,3}
[HW] Hardware				
[Mimp]Medios de impresión	{3,1}	{1,5}	{2,8}	
[Cesc]Computadoras de escritorio	{3,1}	{1,5}	{2,8}	
[Spro]Servidor proxy	{3,1}	{1,5}	{2,8}	
[COM]Redes de Comunicaciones				
[Rlan]Red LAN	{3,1}	{1,5}	{2,8}	{3,3}
[Rwif]Red Wifi	{3,1}	{1,5}	{2,8}	{3,3}
[MEDIA]Soportes de Información				
[Disk]Discos	{2,7}	{3,3}	{3,3}	
[Musb)Memoria USB	{2,7}	{3,3}	{3,3}	
[AUX]Equipamiento Auxiliar				
[Sain]Sistema de alimentación ininterrumpida	{0,63}			
[L]Instalaciones				
[Edif]Edificio	{2,7}	{1,6}	{3,4}	
[P]Personal				
[User]Usuarios Finales	{1,2}	{2,7}	{3,7}	

Tabla 21: Riesgo Potencial
Fuente: Proyecto DPSICIT-UNP – Pilar 5.4.7.

4.3.1.4.2.2 Riesgo Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual.

ACTIVOS	[D]	[I]	[C]	[A]
[S] Servicios				
[telf.] Telefonía Ip.	{2,5}	{2,7}	{2,5}	{2,7}
[inte] Internet	{3,1}	{2,7}	{3,1}	{2,7}
[SW] Software				
[Siaf]Sistema Integrado de Administración Financiera.	{2,5}	{2,7}	{2,5}	{2,1}
[Siga]Sistema Integrado de Gestión Académico.	{2,5}	{2,7}	{2,5}	{2,1}
[Sgad]Sistema de Gestión Administrativa.	{2,5}	{2,7}	{2,5}	{2,1}
[Stdo]Sistema de Tramite documentario.	{2,5}	{2,7}	{2,5}	{2,1}
[Saba]Sistema de Abastecimientos.	{2,5}	{2,7}	{2,5}	{2,1}
[Scap]Sistema de Control de Asistencia del personal.	{2,5}	{2,7}	{2,5}	{2,1}
[Sbpr]Sistema de Banco de Preguntas.	{2,5}	{2,7}	{2,5}	{2,1}
[Sgdo] Sistema de Gestión Docente	{2,5}	{2,7}	{2,5}	{2,1}
[HW] Hardware				
[Mimp]Medios de impresión	{3,1}	{2,7}	{3,1}	{2,7}
[Cesc]Computadoras de escritorio	{3,1}	{2,7}	{3,1}	{2,7}
[Spro]Servidor proxy	{3,1}	{3,3}	{3,7}	{2,7}
[COM]Redes de Comunicaciones				
[Rlan]Red LAN	{3,1}	{2,7}	{2,5}	{2,1}
[Rwif]Red Wifi	{2,5}	{3,3}	{3,1}	{2,7}
[MEDIA]Soportes de información				
[Disk]Discos	{3,1}	{2,2}	{3,1}	{2,7}
[Musb)Memoria USB	{3,1}	{3,3}	{3,1}	{3,3}
[AUX]Equipamiento Auxiliar				
[Sain]Sistema de alimentación ininterrumpida	{3,1}	{3,3}	{3,1}	{3,3}
[L]Instalaciones				
[Edif]Edificio	{3,1}	{3,3}	{3,1}	{2,7}
[P]Personal				
[User]Usuarios Finales	{3,1}	{3,3}	{3,1}	{2,7}

Tabla 22: Riesgo Residual.

Fuente: Proyecto DPSICIT-UNP – Pilar 5.4.7.

4.3.1.4.3 Interpretación de los resultados

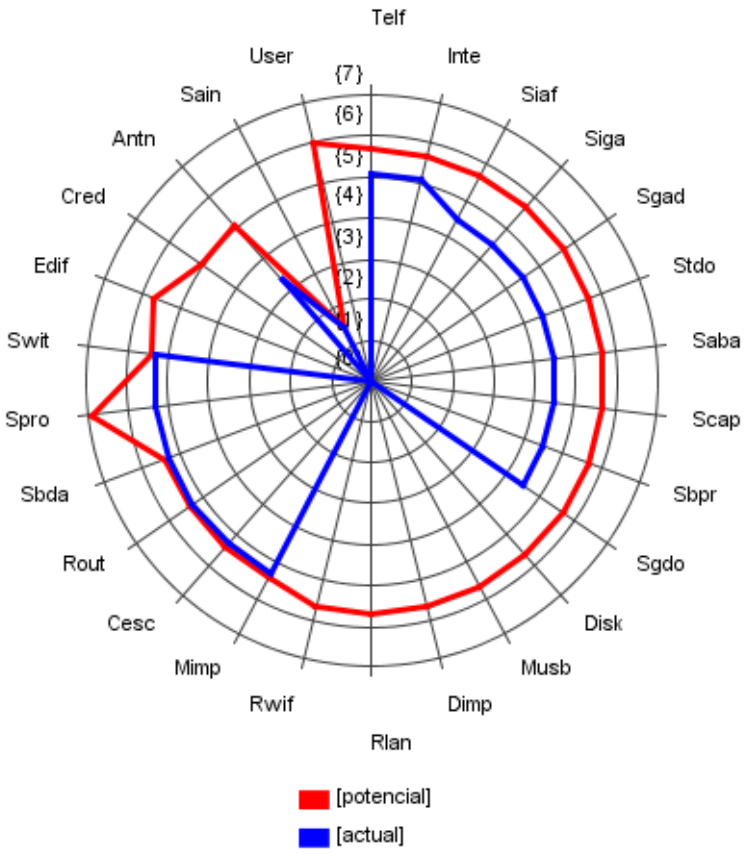


Gráfico 7: Identificación de Riesgos.

Fuente: Pilar 5.4.7.

En la figura se observa, el resultado de todas las actividades que se trabajan sobre los activos, las amenazas y las salvaguardas. Como indica la leyenda, la línea de color rojo son los riesgos que están expuestos los activos, en la siguiente etapa representada por la línea azul es el resultado de la aplicación de las salvaguardas existentes, teniendo en consideración que se maximiza la presencia de amenazas para realizar un estudio de la situación actual en la que se encuentra el objeto de estudio.

4.3.2 Proceso de Gestión de Riesgos

Después de haber realizado el análisis de riesgos queda a la vista los impactos y los riesgos a los que está expuesta la organización.

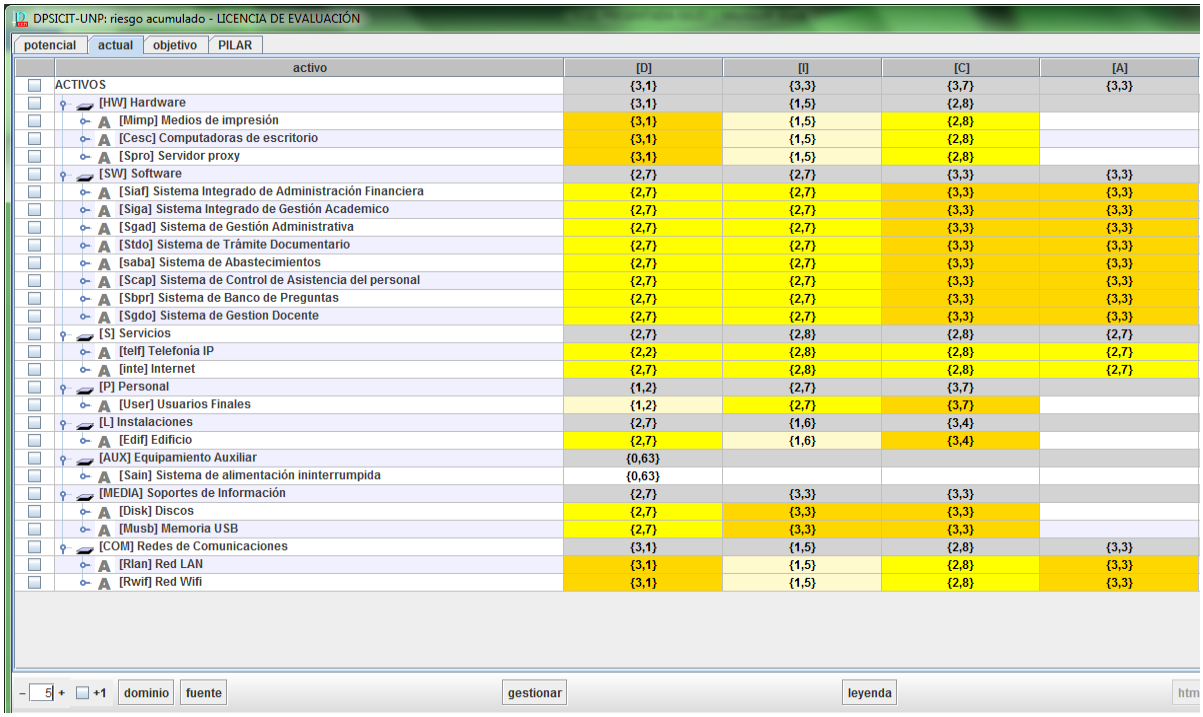
Lo que ha llegado a una calificación de cada riesgo significativo, determinándose si:

- Es crítico en el sentido de que requiere atención urgente.
- Es grave en el sentido de que requiere atención.
- Es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento.
- Es asumible en el sentido de que no se van a tomar acciones.

4.3.2.1 Toma de Decisiones

4.3.2.1.1 Identificación de Riesgos Críticos:

En toda organización los activos están expuestos a riesgos, pero lo importante es conocer cuáles de los activos poseen mayor nivel de riesgo con el fin de implementar salvaguardas para evitar que las amenazas se materialicen. Una vez evaluado los activos y conocido el riesgo a los que están expuestos los mismos, hemos seleccionado los activos que poseen un nivel de riesgo mayor, mostrados a continuación:



activo	[D]	[I]	[C]	[A]
ACTIVOS	{3,1}	{3,3}	{3,7}	{3,3}
[HW] Hardware	{3,1}	{1,5}	{2,8}	
[Mimp] Medios de impresión	{3,1}	{1,5}	{2,8}	
[Cesc] Computadoras de escritorio	{3,1}	{1,5}	{2,8}	
[Spro] Servidor proxy	{3,1}	{1,5}	{2,8}	
[SW] Software	{2,7}	{2,7}	{3,3}	{3,3}
[Siaf] Sistema Integrado de Administración Financiera	{2,7}	{2,7}	{3,3}	{3,3}
[Siga] Sistema Integrado de Gestión Academico	{2,7}	{2,7}	{3,3}	{3,3}
[Sgad] Sistema de Gestión Administrativa	{2,7}	{2,7}	{3,3}	{3,3}
[Stdo] Sistema de Trámite Documentario	{2,7}	{2,7}	{3,3}	{3,3}
[saba] Sistema de Abastecimientos	{2,7}	{2,7}	{3,3}	{3,3}
[Scap] Sistema de Control de Asistencia del personal	{2,7}	{2,7}	{3,3}	{3,3}
[Sbpr] Sistema de Banco de Preguntas	{2,7}	{2,7}	{3,3}	{3,3}
[Sgdo] Sistema de Gestion Docente	{2,7}	{2,7}	{3,3}	{3,3}
[S] Servicios	{2,7}	{2,8}	{2,8}	{2,7}
[telf] Telefonia IP	{2,2}	{2,8}	{2,8}	{2,7}
[inte] Internet	{2,7}	{2,8}	{2,8}	{2,7}
[P] Personal	{1,2}	{2,7}	{3,7}	
[User] Usuarios Finales	{1,2}	{2,7}	{3,7}	
[L] Instalaciones	{2,7}	{1,6}	{3,4}	
[Edif] Edificio	{2,7}	{1,6}	{3,4}	
[AUX] Equipamiento Auxiliar	{0,63}			
[Sain] Sistema de alimentación ininterrumpida	{0,63}			
[MEDIA] Soportes de Información	{2,7}	{3,3}	{3,3}	
[Disk] Discos	{2,7}	{3,3}	{3,3}	
[Musb] Memoria USB	{2,7}	{3,3}	{3,3}	
[COM] Redes de Comunicaciones	{3,1}	{1,5}	{2,8}	{3,3}
[Rlan] Red LAN	{3,1}	{1,5}	{2,8}	{3,3}
[Rwif] Red Wifi	{3,1}	{1,5}	{2,8}	{3,3}

Gráfico 8: Identificación de Riesgos Críticos (Actual)

Fuente: Pilar 5.4.7.

4.3.2.1.2 Calificación del Riesgo:

A continuacion se gestionan los activos con riesgos criticos:

- **Telefonía IP:** este activo pertenece a la capa de Servicios Internos, una vez encontrado amenazas y de haber escogido las salvaguardas antes mencionadas se ha obtenido los siguientes resultados, siendo las amenazas de mayor relevancia:
    - La averia de origen físico y lógico.
    - Fallo de servicio de comunicaciones.

  Las cuales afectan en la Integridad y Confidencialidad(2,8), si se llega a materializar esta amenaza no podrian ejecutar tareas distintas como: Comunicación entre áreas muy distantes de la institución, envío de información de suma importancia mediante este activo.

  Las medidas para reducir el riesgo actual de este activo, son las siguientes:

    - La medida que se debe de tomar es el uso de un manual para el adecuado uso de este activo para así no poder averiarlo de manera física ni lógica, así como además tener constantes charlas para un mejor uso del mismo.

- **Internet:** Este activo pertenece a la capa de servicios internos, una vez encontrado amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados, siendo las amenazas de mayor relevancia:
    - La averia de origen físico y lógico.
    - Fallo de servicio de comunicaciones.

  Las cuales afectan en la la Integridad y Confidencialidad(2,8), si se llega a materializar esta amenaza no podrian ejecutar tareas distintas como: el envio de emails, la gestión de la Pagina Principal de la UNP, el uso de los distintos sistemas de información, etc.

  Las medidas para reducir el riesgo actual de este activo, son las siguientes:

    - La restricción de páginas como son redes sociales, descargar programas. Para que el uso de Internet solo

sea para actividades de trabajo y no para distracciones de empleados(en este caso personal administrativo).

- **Sistema Integrado de Administracion Financiera**
- **Sistema Integrado de Gestion Académico**
- **Sistema de Gestión Administrativa**
- **Sistema de Trámite Documentario**
- **Sistema de Abastecimientos**
- **Sistema de Control de Asistencia de Personal**
- **Sistema de Banco de Preguntas**
- **Sistema de Gestion Docente**

Pertenecientes a la capa de aplicaciones, una vez encontrado amenazas y haber escogido los salvaguardas antes mencionados se han obtenido los siguientes resultados, siendo las amenazas de mayor relevancia:

- Averia de origen físico y lógico.
- Suplantación de identidad.

Las cuales afectan en la disponibilidad(2,7), integridad(2,7), confidencialidad(3,3), autenticidad de los usuarios y la información(3,3), si se llegaran a materializar estas amenazas la oganización podría ser victima de robo de información o de generar datos erroneos en la información perjudicando el desempeño de las actividades de la mayoria de empleados.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- Mejorar la protección de la aplicación con privilegios de acceso de acuerdo al puesto de trabajo y a la información que maneja.

- **Medios de Impresión:** Este activo pertenece a la capa de hardware, una vez encontrado amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados, siendo las amenazas de mayor relevancia:

  - Denegación de servicio
  - Ataque destructivo

  Las cuales afectan en la disponibilidad(3,1), esto es debido a que es muy comun que cualquier persona puede ingresar al

CIT e incluso a alguna oficina pudiendo provocar este tipo de amenazas que afectarían la impresión de papel con información importante para la institución así como también las averías inoportunas por un uso inadecuado.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- La restricción de personas no autorizadas a las oficinas del CIT.

- **Computadora de Escritorio**: Este activo pertenece a la capa de hardware, una vez encontrado amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados, siendo las amenazas de mayor relevancia:

  - Denegación de servicio.
  - Ataque destructivo.

  Las cuales afectan en la disponibilidad(3,1), estas amenazas son muy comunes ya que algunos empleados no teniendo un conocimiento de cómo solucionar algun problema que ocurra en el computador ellos mismo intentan darle una solución sin tomar las precauciones del caso, terminando por averiar el activo, en incluso provocando que no pueda comunicarse mediante la red de trabajo.

  Las medidas para reducir el riesgo actual de este activo, son las siguientes:

  - En caso de fallo de alguna computadora de escritorio, llamar a personal de informática para que pueda solucionar el problema.

- **Servidor Proxy:** Este activo pertenece a la capa de hardware, una vez encontrado amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados, siendo las amenazas de mayor relevancia:

  - Suplantación de la identidad.
  - Denegacion de servicio.
  - Ataque destructivo.

Las cuales afectan en la disponibilidad(3,1),integridad de los datos(1,5),confidencialidad de los datos(2,8), estas amenazas se puedan dar debido a que no existen medidas de seguridad informática en donde los hackers pueden obtener acceso no autorizados mediante la suplantación de identidad.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- Creación del área de seguridad de la información.

- **Personal:** Que son todo el personal administrativo que se encuentra en la organización, las principales amenazas que posee el personal que labora en esta empresa son la ingenieria social y extorsión.
  La primera amenaza se cumple por que los empleados saben la clave de los demas para acceder a su computador de esta manera se puede sustraer, modificar y destruir la información. Originando a que la segunda amenaza que puede ser utilizada como extorsion o como abuso de buena fe para beneficio propio del atacante.
  La medida para reducir el riesgo actual de este activo, es la siguiente:
  - Cear una normativa relativa a la gestion de personal(en materia de seguridad).
  - Crear procedimientos relevantes de seguridad: emergencias, incidencias.
  - Prevención y reacción frente a extorsión.
  - Prevención y reacción frente ataques de ingeniería social.

4.4 Diseño de Plan de Seguridad

4.4.1 Introducción

El presente plan de seguridad de la información tiene como finalidad establecer objetivos de seguridad para la organización.

Este plan consta de dos partes, la primera parte la constituyen: una breve presentación, descripción del objetivo del plan, el alcance del mismo y un resumen de resultados del análisis de riesgo; en la segunda parte se describe cada uno de los objetivos del plan:

- **Elaborar políticas de seguridad informática.**
- **Mejorar la seguridad física.**
- **Mejorar la seguridad lógica.**
- **Mejorar la seguridad en redes.**
- **Implementar estrategias de continuidad.**
- **Revisar el cumplimiento de las políticas de seguridad de la información.**

4.4.2 Primera Parte

4.4.2.1 Presentación

El diseño del plan de seguridad de la información para el Centro de Informática y Telecomunicaciones de la UNP, periodo 2015-2018; responde a los siguientes principios que definen la seguridad informática.

- **Confidencialidad:** Proporcionando acceso a la información solamente a los usuarios autorizados.

- **Integridad:** Garantizando que la información sobre la cual la organización tomará decisiones no haya sufrido manipulación alguna antes, durante y después de su procesamiento.
- **Disponibilidad:** Permitiendo acceder a la información o utilizar algún servicio informático siempre que sea necesitado.

4.4.2.2 Objetivo General

El objetivo es Diseñar un Plan de Seguridad de la Información para proteger los activos informáticos que se utilizan y generan en los procesos de la Universidad Nacional de Piura administrados por el Centro de Informática y Telecomunicaciones.

4.4.2.3 Alcance

Este documento se aplica para los 38 usuarios administrativos del Centro de Informática y Telecomunicaciones de la UNP, así como a personal externo que desempeñen labores o le proporcionen algún tipo de servicio o producto a la organización.

4.4.2.4 Resumen de Resultados del Análisis de Riesgo

De este análisis se determinó que Los sistemas de información: Sistema Integrado de Administración Financiera, Sistema Integrado de gestión Académica, Sistema de Tramite Documentario, Sistema de Gestión Administrativa-Ingresos, Sistema de Abastecimientos, Sistema de Control de Asistencia del Personal, Sistema de Banco de preguntas, Sistema de Gestión Docente (CAPA DE SOFTWARE) están en la categoría de riesgo alto; la Red Lan, Red Wifi (CAPA DE REDES DE COMUNICACION) están categorizados con un riesgo medio, y el edificio (CAPA DE INSTALACIONES) es el activo que tiene un riesgo bajo.

4.4.3 Segunda Parte

Para el desarrollo del Plan de Seguridad de la Información se ha establecido 6 objetivos, en donde el primer y el segundo objetivo se desarrollarán en los meses de Julio y Agosto; el tercero y Cuarto se llevará a cabo en el mes de

Septiembre; el Quinto se efectuará en el mes de Octubre; el Sexto será cada seis meses a partir de la ejecución de este plan.

4.4.3.1 Objetivo 1-Elaborar Políticas de Seguridad Informática

Tareas

a. Se debe identificar los riesgos de la organización siguiendo una metodología de riesgo.
b. Se debe seguir las tareas de la metodología Magerit: Caracterización de los Activos, Caracterización de las Amenazas, Caracterización de las Salvaguardas, Estimación del estado de riesgo
c. Se documenta la política, alineada con los objetivos generales de la organización y basada en modelos de tecnología de la información.
d. Se capacita a todo el personal en materia de seguridad y en la política.
e. Se implementa la política

Responsables

El Jefe de Seguridad Informática si lo hubiera y el Director del CIT serán los encargados del cumplimiento de este objetivo que será ejecutado por toda la organización.

Fecha de Realización

Mes de Julio y Agosto.

4.4.3.2 Objetivo 2- Mejorar la Seguridad Física

Tareas

a. Establecer un sistema biométrico de registro de acceso al centro de procesamiento de datos.
b. Se comprarán e instalarán equipos de seguridad definidos con el director de CIT (cámaras de seguridad, alarmas contra robo, extintores, sistema de detección de humo, etc.)
c. Se llevará registros del mantenimiento preventivo y correctivo que se realice a los equipos de computación.
d. Se capacitará al personal en las medidas de seguridad física.

Responsables

El Jefe de Seguridad Informática si lo hubiera, el Director del CIT y el encargado de compras (almacenero) serán los encargados de la ejecución de este objetivo el cual se llevará a cabo en toda la organización.

Fecha de Realización

Mes de Julio y Agosto.

4.4.3.3 Objetivo 3- Mejorar la Seguridad Lógica

Tareas

a. Establecer que el tiempo de conexión de la red se limite al horario normal de oficina.
b. Llevar una bitácora de eventos que incluya:
    a. El identificador del usuario.
    b. Fecha, hora de conexión y desconexión.
    c. Registro de los intentos aceptados y rechazados de acceso al sistema, datos y otros recursos.
c. Se capacitará al personal en las medidas de seguridad lógica.

Responsables

El Jefe de Seguridad Informática si lo hubiera y el director del CIT serán los encargados de la ejecución de este objetivo en los sistemas de información de la organización.

Fecha de Realización

Mes de Septiembre.

4.4.3.4 Objetivo 4- Mejorar la Seguridad en Redes

Tareas

a. Capacitar a los usuarios en el uso de software antivirus y en las precauciones adecuadas en el uso del correo electrónico.
b. Realizar periódicamente escaneos de virus a los equipos.
c. Actualizar el antivirus en los computadores ya sea como control preventivo o como rutina básica de seguridad.
d. Programar el firewall para dar accesos de acuerdo a las funciones y direcciones IP de los usuarios.

Responsables

El jefe de Sistemas será el responsable de llevar a cabo este objetivo en toda la organización.

Fecha de Realización

Mes de Septiembre.

4.4.3.5 Objetivo 5-Implementar Estrategias de Continuidad

Tareas

a. Se instalarán fuentes de poder ininterrumpibles (UPS).
b. Seleccionar un centro alternativo y almacenamiento externo.
c. Definir y seleccionar un acuerdo contractual para los servicios de continuidad de la organización.
d. Se realizarán respaldos diarios de la información de la Base de Datos.
e. El Jefe de Seguridad Informática si lo hubiera en conjunto con el director del CIT, determinarán el lugar donde se guardarán los respaldos fuera de la Institución.

Responsables

El jefe de Sistemas y El Jefe de Seguridad Informática si lo hubiera serán los responsables de llevar a cabo este objetivo en toda la organización.

Fecha de Realización

Mes de Octubre.

4.4.3.6 Objetivo 6-Revisar el Cumplimiento de las Políticas de seguridad de Información

Tareas

a. Los sistemas de información serán revisados para la conformidad con los estándares de implementación de seguridad.

b. Los jefes de Área se asegurarán de que se cumplen correctamente los procedimientos de seguridad dentro de su área de responsabilidad.

c. Todas las áreas de la organización serán consideradas para las revisiones regulares del cumplimiento de las políticas de seguridad.

Responsables

El Jefe de Seguridad Informática si lo hubiera y el Director del CIT serán los encargados de hacer cumplir este objetivo en toda la organización.

Fecha de Realización

Cada seis meses a partir del inicio de la ejecución de este plan.

4.4.4 Calendarización

Meses	Julio				Agosto				Septiembre				Octubre				Noviembre			
tareas/tiempo(semanas)	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.-Elaborar politicas de seguridad informática																				
tarea a																				
tarea b																				
tarea c																				
tarea d																				
tarea e																				
2.-Mejorar seguridad Fisica																				
tarea a																				
tarea b																				
tarea c																				
tarea d																				
3.-Mejorar seguridad Logica																				
tarea a																				
tarea b																				
tarea c																				
4.-Mejorar seguridad en Redes																				
tarea a																				
tarea b																				
tarea c																				
tarea d																				
5.-Implementar estrategias de continuidad																				
tarea a																				
tarea b																				
tarea c																				
tarea d																				
tarea e																				
6.-Revisar el cumplimiento de las politicas de seguridad de la informacion																				
tarea a																	A partir de aquí cada 6 meses			
tarea b																				
tarea c																				

Tabla 23: Calendarización

4.4.5 Financiamiento

Mecanismos de seguridad	Características	Descripción	Cantidad	Costo Unitario	Costo total
Sistema biométrico.	Reconocer los rasgos combinados tanto de huella como facial para controlar el ingreso de personas autorizadas al centro de procesamiento de datos	Ingreso al edificio (1er Piso). Ingreso a lugares autorizados (DATA CENTER). 4to Piso	2	1300	S/. 2,600.00
Sistema de Videovigilancia	Mediante este dispositivo se tendrá un registro de las actividades de los empleados que laboran en el centro de procesamiento de datos.	Ingreso y egreso de personal y externos. Reconocimiento Facial. Movimiento (infrarrojo) . 1 cámara por Piso	5	156	S/. 780.00
Antivirus	Permite detectar software malicioso, filtros antipishing para detectar intentos de suplantación de páginas, etc.	Antivirus Corporativo, que permitirá instalar el antivirus a cada cliente, actualizándolo automáticamente. Se encontrará en toda la red	-	-	S/. 36,000.00
Firewall	Ayuda a detectar actividad sospechosa o evasiva dentro de la red de la institución	Firewall Demarcador - Exinda 4010, toda la red	-	-	
Backup.	Ayuda a hacer una copia de los datos originales con el fin de disponer de un medio para recuperarlos en caso de su perdida	Almacenamiento de 40 Tb en la nube, toda la red	-	-	
UPS(fuentes de poder ininterrumpibles).	Permitirá dar energía por un tiempo prudente para que el trabajador tenga el tiempo necesario para guardar archivos de importancia y apagar el ordenador de forma correcta en caso de un corte de luz o un problema eléctrico.	UPS para Servidor (Biblioteca central). UPS para Data Center UPS para oficina de administrativos.	20	455	S/. 9,100.00
Sistema de detección de humo-incendio	Para la detección y previsión de siniestros a causa del fuego.	En Oficinas administrativas del CIT	1	S/. 2,900.00	S/. 2,900.00
Extintores	Artefactos que permiten controlar un amague de incendio	En Oficinas administrativas del CIT de tipo CO2-PQS(9KG)	5	S/. 110.00	S/. 550.00
TOTAL					**S/. 51,930.00**

Tabla 24:Financiamiento

4.4.6 Presupuesto

RUBROS	MONTO
RR.HH	
Auditor	S/. 1,500.00
Analista Junior	S/. 500.00
TOTAL DE RR.HH	S/. 2,000.00
BIENES	
Fotocopias	S/. 100.00
Movilidad	S/. 500.00
Viáticos	S/. 150.00
Impresiones	S/. 250.00
TOTAL DE BIENES	S/. 1,000.00
SERVICIOS	
Internet	S/. 600.00
Servicios no Personales	S/. 800.00
Consumo de Energía	S/. 500.00
TOTAL DE SERVICIOS	S/. 1,900.00
FINANCIAMIENTO DE MECANISMOS DEL PLAN	
TOTAL FINANCIAMIENTO	S/. 51,930.00
OTROS	
Algunos Imprevistos	S/. 300.00
TOTAL DE OTROS	S/. 300.00
TOTAL	**S/. 57,130.00**

Tabla 25: Presupuesto

4.5 Modelo de Seguridad de la Información

Luego de haber concluido el análisis de riesgo al centro de procesamiento de datos procedemos a diseñar un modelo de seguridad de la información de acuerdo a la institución y sus recursos informáticos.

El objetivo de este modelo de seguridad es la de establecer un marco para la implantación de seguridad y control que abarque a todas las áreas de la organización mediante políticas.

Esta política cubrirá las siguientes secciones:

- Justificación.
- Generalidades.
- Seguridad Física.
- Seguridad Lógica.
- Seguridad en Redes

4.5.1 Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de toda compañía; esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, intrusos, hackers, accidentes, desastres naturales, etc.

La información debe protegerse de acuerdo a su valor e importancia empleándose medidas de seguridad sin importar como la información se guarda (en papel o en forma electrónica), o como se procesa (PC’s, servidores, etc.), de igual manera en cómo se transmite (correo electrónico, conversación telefónica), tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.

4.5.2 Generalidades

Esta política debe ser comunicada a todos los usuarios de la institución, de una forma apropiada, accesible y entendible para el lector.

4.5.3 Objetivo

La institución debe tener vigente una política de seguridad informática que le permita establecer un marco para la implantación de seguridad y control extensivo a todas las áreas.

4.5.4 Alcance

Esta política se aplica a toda la institución, rige para todos los empleados de sistemas y personal externo.

4.5.5 Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la Seguridad de la información en el Centro de Informática y Telecomunicaciones de la UNP

a) **Comité de Informática.** -Estará conformado por el Jefe de CIT, Jefe de Seguridad Informática si lo hubiera y el Jefe de Sistemas, este comité será responsable de implantar y velar por el cumplimiento de las políticas, normas, pautas, procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Coordinación Administrativa del CIT-UNP.

También es responsable de evaluar, adquirir e implantar productos de seguridad informática, realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

b) **Jefe de Seguridad Informática. -**Es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad de la Información, así como recomendar las medidas pertinentes.

c) **Jefe de Sistemas. -**Es responsable de establecer los controles de acceso apropiados para cada usuario, la creación de nuevos usuarios, supervisar el uso de los recursos informáticos, administrar la red, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra; también es responsable de informar al Jefe de Seguridad de la Información y a sus superiores sobre toda actividad sospechosa o evento insólito.

d) **Usuarios.** -Son responsables de cumplir con todas las políticas de la institución relativas a la seguridad informática

4.5.6 Incumplimiento o Violación de las políticas

Si se llegase a incumplir o violar una de estas políticas por parte del personal, el área de sistemas o seguridad informática si existiere, se realizará un informe detallado, el cual describirá la circunstancia y la gravedad del hecho y el Rector de la Universidad deberá tomar las medidas necesarias sobre la(s) persona(s) implicada(s).

4.5.7 Estructura de la política

Esta política se divide en las siguientes secciones:

- Seguridad Física
- Seguridad Lógica
- Seguridad en Redes

Cada sección se divide en tres partes:

Propósito: Define la intención en cada sección.
Alcance: Define el ámbito de aplicación.
Controles Generales: Define los objetivos para cada sección.

4.5.8 Política de Seguridad Física

a) Propósito

El propósito de esta política es preservar la seguridad de los recursos informáticos, garantizar la integridad y disponibilidad de los mismos

b) Alcance

Estas políticas son aplicables a todos los recursos informáticos de la institución entendiendo por ellos: hardware, personal e instalaciones.

c) Controles Generales

- Las computadoras de la institución solo deben usarse en un ambiente seguro, se considera que las oficinas del CIT son un ambiente seguro porque en ellas se han implantado las medidas de control apropiadas para proteger datos, hardware, software, personal e instalaciones.
- Toda persona debe portar credenciales de identificación.

- El personal de vigilancia debe controlar el ingreso y egreso de vehículos llevando una planilla con los datos personales de los ocupantes, la marca, número de placa, la hora de entrada y salida del mismo.
- Se debe mantener registros de entrada al centro de cómputo.
- Se debe instalar videocámaras en el CIT-UNP a fin de identificar personas ajenas a la organización.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el departamento de Sistemas, pues este cambio puede poner en riesgo la integridad y disponibilidad del equipo.
- Se debe contar con señalización de salidas de emergencia, prohibiciones de beber, fumar o comer alrededor de los equipos.
- Se debe contar con una libreta donde se encuentren teléfonos de emergencia, para cualquier contingencia.
- Deben usarse reguladores de voltaje, equipos de protección como fuentes de poder ininterrumpibles (UPS).
- Instalar alarmas en el centro de cómputo, así como detectores de humo como esquemas correctivos ante incendios.
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como perdida de la información o indisponibilidad de los servicios.
- Los servidores de red y los equipos de comunicación (módems, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo; debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

4.5.9 Política de Seguridad Lógica

a) Propósito

Tiene como propósito controlar el acceso a la información y los procesos de la organización.

b) Alcance

Estas políticas son aplicables para todos los sistemas de información, datos de la institución, software. Así mismo es aplicable a todos los miembros de la entidad que hacen uso de los sistemas de información.

c) Controles Generales

i. Cuentas

- Se debe crear un documento en donde el empleado del CIT declare conocer las políticas, procedimientos de seguridad y se haga responsable del uso de su cuenta de usuario.
- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada por el respectivo Jefe de Área y el director del CIT.
- Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
- Los privilegios de lectura, escritura, creación, eliminación y modificación de datos deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- Cuando un empleado es despedido, renuncia o sale de vacaciones del centro de procesamiento de datos, debe desactivarse su cuenta antes que deje el cargo.
- La cuenta de un usuario es personal e intransferible, por lo cual no se permite que este comparta su cuenta ni su contraseña con persona alguna, aun si está acreditada la confianza del usuario.

ii. Contraseña

- La longitud de la contraseña serán de mínimo 8 caracteres y máximo 10(entre letras y números).
- No deben ser utilizadas como claves los datos personales y acrónimos.
- El usuario no debe guardar su contraseña en una forma legible en archivos, disco, USB u otros dispositivos, tampoco debe escribirla en papel o dejarla en sitios donde pueda ser encontrada.
- Nunca debe compartirse la contraseña o revelarla a otros.
- Las contraseñas deben ser encriptadas para imposibilitar su identificación.

iii. Control de Acceso

- Al momento de ingresar al sistema de información y sistema operativo al que tienen permiso cada usuario en el CIT se deberá notificar la fecha, hora y dirección desde la que se conectó al sistema por última vez.
- Para prevenir ataques al software debe limitarse a 3 el número de intentos consecutivos de introducir la contraseña, luego de lo cual la cuenta involucrada quedará suspendida y se alertará al Administrador del Sistema.
- Si no existiera alguna actividad en un terminal, PC o estación de trabajo hasta un tiempo máximo 30 minutos, el sistema debe automáticamente apagar la pantalla y suspender la sesión.
- Los usuarios no deben violar los sistemas de seguridad y control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas del CIT, siendo causal de despido.

iv. Aplicaciones

- Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como programas u herramientas

que rastrean vulnerabilidades en sistemas de cómputo propios o ajenos.

- Se deben generar registros de:
  - El identificador del usuario.
  - Fecha y hora de conexión y desconexión al sistema.
  - Intentos aceptados y rechazados de acceso al sistema.
- Los archivos de bitácora (logs) y los registros de auditoria que graban los eventos relevantes sobre la seguridad de los sistemas informáticos, deben revisarse cada semana y guardarse durante un tiempo prudencial de por lo menos 3 meses.
- Está prohibido instalar programas de uso personal.

4.5.10 Política de Seguridad en Redes

a) Propósito

El propósito de esta política es establecer los procedimientos y los requisitos para asegurar la protección apropiada de la compañía al estar conectada a redes de computadoras.

b) Alcance

Esta política se aplica a todos los empleados y personal temporal de la organización.

c) Controles Generales

Correo electrónico, Internet e Intranet

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada, al detectarse presencia de un virus u otro agente potencialmente peligroso se debe notificar al Jefe de Sistemas
- No debe descargarse software del internet y en general que provenga de una fuente no confiable, al menos que este haya sido comprobado en forma rigurosa y que esté aprobado por el Área de Sistemas.

- Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades laborales
- No ingresar a páginas externas que no sean de uso de la UNP.
- El firewall será programado para dar acceso solo a páginas que cada usuario por sus funciones tendrá permitido acceder.

4.6 Plan de Recuperación ante un Desastre y Respaldo de la Información

El paso inicial ante el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones, estas personas pueden ser: personal del CIT, personal de Seguridad.

Las actividades a realizar en un plan de Recuperación de Desastres se clasifican en tres etapas:

- ❖ Actividades Previas al Desastre.
- ❖ Actividades Durante el Desastre.
- ❖ Actividades Después del Desastre.

4.6.1 Actividades previas al desastre

Se considera las actividades de planeamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguraran un proceso de recuperación con el menor costo posible para la organización.

4.6.1.1 Establecimiento del Plan de Acción

En esta fase de planeamiento se establece los procedimientos relativos a:

a. Equipos de Cómputo.
b. Obtención y almacenamiento de los respaldos de Información (Backups).

a. Equipos de Computo

Se debe tener en cuenta el catastro de Hardware, impresoras, lectoras, scanner, plotters, módems, fax y otros, detallando su ubicación (software que se usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos

- Pólizas de seguros comerciales, como parte de la protección de los activos y considerando una restitución por equipos de mayor potencia.
- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación.
- Mantenimiento actualizado del inventario de los equipos de cómputo.

b. Obtención y almacenamiento de Copias de Seguridad(Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la organización. Las copias de seguridad son las siguientes:

- Backup del Sistema Operativo: o de todas las versiones de sistema operativo instalados en la Red.
- Backup de Software Base: (Lenguajes de Programación utilizados en el desarrollo de los aplicativos institucionales).
- Backup de los datos (Base de datos, password y todo archivo necesario para la correcta ejecución del software).
- Backups del hardware: se puede implementar bajo dos modalidades.

Modalidad Externa: Mediante el convenio con otra institución que tenga equipos similares o mejores y que brinden la capacidad y seguridad de procesar nuestra información y ser puesta a nuestra disposición.

Modalidad Interna: Si se dispone de más de un local, en ambos se debe tener señalado los equipos, que por sus capacidades técnicas pueden ser usados como equipos de emergencia.

4.6.1.2 Formación de Equipos Operativos

En cada unidad operativa, que almacene información y sirva para la operatividad de la organización, se deberá designar un responsable de la seguridad de la información de su unidad, debiendo ser el Jefe Administrativo de dicha Área, sus funciones serán las siguientes:

- Contactarse con los autores de las aplicaciones y personal de mantenimiento respectivo.
- Proporcionar las facilidades (procedimientos, técnicas) para realizar copias de respaldo.

Las siguientes actividades estarán dirigidas por el equipo de soporte y mantenimiento:

- Supervisar el procedimiento de respaldo y restauración.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software: el encargado y el usuario final dan su conformidad.
- Ejecutar trabajos de recuperación y comprobación de datos.

4.6.1.3 Formación de Equipos de Evaluación (Auditoria de cumplimiento de los procesos de seguridad)

Esta función debe ser realizada de preferencia por una entidad externa de auditoria, en donde se debería:

- Revisar que las normas y procedimientos con respecto a backups, seguridad de equipos y data se cumpla.
- Supervisar que la realización de los backups se haya hecho de manera periódica, por parte de los que conforman el equipo operativo.
- Revisar la correlación entre la relación de los sistemas e información necesarios para la buena marcha de la institución y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las normas para las acciones de correcciones necesarias.

4.6.2 Actividades durante al desastre

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades:

a. Plan de emergencias
b. Formación de equipos
c. Entrenamiento.

a. Plan de emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada.

Solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de las personas

Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención ante desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del desastre cause más daños o destrucciones, todo el personal debe conocer lo siguiente:

- Localización de vías de Escape o Salida: Las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina debe señalizar las vías de escape.

- Plan de evacuación personal: El personal ha recibido periódicamente instrucciones para evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local.

- Ubicación y señalización de los elementos contra el siniestro: Tales como los extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde.

- Secuencia de llamadas en caso de siniestro: Tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

b. Formación de equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastres, en caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.) se debe formar 02 equipos de personas que actúen directamente durante el

siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos.

c. Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos.

4.6.3 Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

a. Evaluación de daños.
b. Priorización de Actividades del Plan de Acción
c. Ejecución de Actividades
d. Evaluación de resultados.
e. Retroalimentación del Plan de Acción

a. Evaluación de Daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo.

En el caso de la UNP se debe atender los procesos de contabilidad, tesorería, administrativo-académicos, documentarios; que son las actividades que no podrían dejar de funcionar

b. Priorizar actividades del plan de Acción.

La evaluación de los daños reales nos data una lista de las actividades que debemos realizar; las actividades comprenden la recuperación y

puesta en marcha de los equipos de cómputo y los sistemas de información, compra de accesorios dañados, etc.

c. Ejecución de Actividades.

Se deberá contar con equipos de trabajo en donde cada uno deberá tener un coordinador quien reportará el avance de los trabajos de recuperación, en caso de producirse un problema reportarlo de inmediato a la Jefatura.

Los trabajos de recuperación tendrán dos etapas:

- La primera la restauración del servicio usando los recursos de la institución o local de respaldo.
- La segunda etapa es volver a contar con los recursos en la cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

d. Evaluación de resultados

Una vez concluidas las labores de recuperación de los activos que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del Plan de Acción, como se comportaron los equipos de trabajo, etc.

CONCLUSIONES

- Con el uso del estandar de seguridad de la informacion ISO 17799, se logra diseñar el Plan de Seguridad de la Información mediante la aplicación de las tareas mencionadas en este proyecto para lograr los siguientes objetivos:**Elaborar politicas de seguridad informatica,Mejorar seguridad fisica,Mejorar seguridad logica,Mejorar seguridad en Redes,Implementar estrategias de continuidad,Revisar el cumplimiento de las políticas de seguridad** permitiendo así una mejor protección de los activos informaticos que se utilizan y generan en cada uno de los procesos de la UNP, donde no se contaba con un plan de seguridad.

- Como resultado de la aplicación de la metodologia Magerit y herramienta Pilar, se concluye que el CIT está expuesto a una serie de riesgos que son críticos para su funcionamiento mediante amenazas como: **difusion de software dañino, acceso no autorizado**; las cuales son muy probables que ocurran lo cual sustenta la problemática expuesta y la importancia del desarrollo de este proyecto, por lo cual este trabajo será de gran beneficio para minimizar riesgos que generan incidencias en el resguardo de la información.

- Mediante el **Modelo de Seguridad de la información** en el CIT de la UNP se logra crear en los trabajadores una cultura de seguridad informática a través de politicas, por ende se tendrá un mejor resguardo de la informacion en el centro de procesamiento de datos.

- Se elaboró un **Plan de recuperación ante un desastre y respaldo de la información,** en caso de que un evento fuera de su alcance pueda ocasionar una interrupción parcial o total en sus funciones al centro de procesamiento de datos.

RECOMENDACIONES

- El centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura deberá realizar un análisis de riesgo cada cierto tiempo, este periodo de tiempo deberá establecerse según el impacto de riesgo en el que se encuentre la organización.

- Debería de existir un área de seguridad informática en donde el personal encargado deberá monitorear constantemente los distintos incidentes de seguridad.

- Capacitar al personal para que se cumplan las políticas de seguridad de la información establecidas.

BIBLIOGRAFIA

Garcia, D., & Villegas, R. (2014). *Seguridad informática basado en las normas y estandares internacionales COBIT e ISO 17799*. http://www.monografias.com/trabajos101/seguridad-informatica-basado-normasy-estandares-internacionales-cobit-e-iso-17799/seguridad-informatica-basado-normasy-estandares-internacionales-cobit-e-iso-17799.shtml

Guevara Chumán, Javier Gustavo. (2015). *Aplicación de la Metodología Magerit para el Análisis y Gestión de Riesgos en los Servidores de los Sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo.pdf.* Universidad Nacional Pedro Ruiz Gallo.

Hernandez Pinto, María Gabriela. (2006). *Diseño de un Plan Estratégico de Seguridad de Información en una Empresa del Sector Comercial.*Universidad Superior Politécnica del Litoral,Guayaquil.

Mañas Argemí, Jose Antonio. (2012). *Manual de Usuario Pilar Basic 5.2.pdf.* https://es.scribd.com/mobile/document/153081679/472C-Manual-de-Usuario-PILAR-BASIC-5-2-Jul12

Monografías. (s.f). *Seguridad Informática*.
http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml#seguridada

Padilla,Cristina. (2012). *Análisis y Gestión de Riesgos Informáticos para la proteccion de los Sistemas de Información en el Area de Tecnologías Informáticas del Gobierno Provincial de Tungurahua.*Universidad Tecnica de Ambato,Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Portal de Administración Electrónica. (2012). *MAGERIT versión 3.pdf*. http://administracionelectronica.gob.es/ctt/magerit#.Vb2R09V_Oko

Portillo, F. (2010). *La Seguridad de la Información*.
http://fportillo.webnode.es/products/la-seguridad-de-la-informacion/

Vanegas M., M. (s.f). *Seguridad Informática*. http://seguridadinformatica201v.blogspot.com/p/principios-de-seguridad-informatica.html

Villalon Huerta, A. (2004). *El Sistema de Gestión de Seguridad de la Información.* http://www.shutdown.es/ISO17799.pdf

ANEXOS

ANEXO I: SISTEMAS DE INFORMACIÓN EN LA UNP, CRÍTICOS PARA LA CONTINUIDAD DE NEGOCIOS.

La relación de los sistemas de información deberá detallar los siguientes datos:

Nombre del Sistema	**Área que genera la información base**	**Áreas que usan la información**	**Volumen de transacciones**	**Equipamiento necesario**	**Fechas en que la información se necesita urgente.**
Sistema Integrado de Administración Financiera (SIAF). Uso obligatorio en Instituciones públicas, por el MEF	La oficina Central de Ejecución Presupuestaria.	OCEP, Oficina de Presupuesto.		Conexión a Internet.	Diario.
Sistema Integrado de Gestión Académico. Desarrollo CIT.	Las oficinas de Secretarias Académicas, OCRCA.	Las Oficinas Académicas, OCRCA, Autoridades Académicas-Administrativas-Control.	Proceso de Inscripción de cursos y Entrega de Actas.	Conexión a Internet.	Diario.
Sistema de Gestión Administrativa –	Todas las Unidades	Todas las Unidades	Descarga diario de los archivos del	Intranet.	Diario.

Ingresos. Desarrollo CIT.	Operativas-Área Administrativa.	Operativas – Oficina Administrativa, Autoridades Administrativas.	banco.		
Sistema de Trámite Documentario.	Todas las Unidades Operativas – Trámite documentario.	Todas las Unidades Operativas – Trámite documentario, Autoridades.	Registro diario de los documentos.	Intranet	Diario.
Sistema de Abastecimientos. Desarrollo Externo	Oficina de Abastecimientos.	Oficina de Abastecimientos.	Registro diario de Órdenes de Trabajo.	Intranet.	Diario.
Sistema de Control de Asistencia del personal. Desarrollo del CIT.	Oficina de Recursos Humanos-Control de Asistencia.	Oficina de Recursos Humanos-Control de Asistencia	Registro diario de las Asistencias de los trabajadores.	Intranet.	Diario.
Sistema de Banco de Preguntas.	Comisión de Exámenes de Idepunp.	Comisión de Exámenes de Idepunp.	Periodo de promedio cada cinco semanas.	Intranet.	Exámenes Admisión UNP/ETSUNP.

Anexo II: ENCUESTA RUBRICA DE VALORES- CRITERIOS DE RIESGO

1.- Actualmente, ¿Su teléfono IP tiene línea?

A) SI B) NO

2.- Siempre que realiza una llamada, ¿al primer intento timbra?

A) SI B) NO

3.- Durante la llamada, ¿Cómo es la calidad de la señal?

A) Excelente B) Buena C) Regular D) Pésima

4.- ¿Siempre posee internet?

A) SI B) NO C) A veces

5.- Cuando empieza a navegar, ¿Accede inmediatamente a la página web referida?

A) SI B) NO C) A veces

6.- ¿Considera seguro administrar su información personal durante la jornada laboral?

A) SI B) NO

7.- ¿Ha notado algún comportamiento raro del navegador mientras se encuentra en internet?

A) SI B) NO C) A veces

Si su PC cuenta con cable para acceder a internet, de lo contrario ir a la pregunta 12

8.- ¿Posee internet estando el cable conectado?

A) SI B) NO C) A veces

9.- ¿Suele mover el cable para que regrese el internet?

A) SI B) NO C) A veces

10.- Cuando recibe un correo, ¿Encuentra inconvenientes en el archivo adjunto?

A) SI B) NO C) A veces

9.- ¿Posee internet estando conectado a la Red Wifi?

A) SI B) NO C) A veces

10.- ¿Suele conectar y desconectar de la red para que regrese el internet?

A) SI B) NO C) A veces

11.- ¿Cómo considera la velocidad de descarga de archivos?

A) Excelente B) Buena C) Regular D) Pésima

12.- ¿Se puede acceder el sistema?

A) SI B) NO C) A veces

13.- ¿Se realizan correctamente sus transacciones?

A) SI B) NO C) A veces

14.- ¿Las transmisiones son correctas con el servidor?

A) SI B) NO C) A veces

15.- ¿La impresora seleccionada, siempre está disponible?

A) SI B) NO C) A veces

16.- ¿Demora en Imprimir después de haber mandado una orden?

A) SI B) NO C) A veces

17.- ¿Tiene problemas con su PC asignada?

A) SI B) NO C) A veces

18.- ¿Su máquina tiene virus?

A) SI B) NO

19.- ¿Puede acceder a redes sociales o YouTube?

A) SI B) NO C) A veces

20.- ¿Su memoria USB tiene virus?

A) SI B) NO C) A veces

21.- ¿La institución cuenta con UPS para servidores?

A) SI B) NO

22.- En caso de que sea afirmativa la pregunta anterior, ¿Funcionan correctamente?

A) SI B) NO C) A veces

23.- ¿Posee medidas de seguridad el edificio?

A) SI B) NO C) A veces

24.- ¿Cada usuario posee una clave para acceder al equipo?

A) SI B) NO C) A veces

25.- ¿Los usuarios cambian sus claves de acceso?

A) SI B) NO C) A veces

Anexo III: EVALUACION SEGURIDAD FISICA

1. ¿Existe un manual documentado de políticas y procedimientos de seguridad física?

   Si ( ) No (X)

2. ¿Existe uno de estos métodos para controlar el acceso a personas ajenas al Centro de procesamiento de datos?

	SI	NO
• Guardias de seguridad	(X)	( )
• Detectores de Metales	( )	(X)
• Sistemas Biométricos	( )	(X)
• Protección Electrónica	( )	(X)

3. ¿Existe uno de estos métodos para controlar el acceso a personas ajenas al área?

	SI	NO
• Puerta con cerradura	(X)	( )
• Puertas sensoriales	( )	(X)
• Videocámaras	( )	(X)
• Escolta controlada Para acceso de visitantes	( )	(X)
• Alarmas	( )	(X)

4. ¿El personal de la institución cuenta con alguna identificación que los diferencie de los visitantes?

   Si ( ) No (X).

5. ¿El centro de procesamiento de datos está alejado de almacenes de materiales peligrosos?

   Si (X) No ( )

6. ¿Está prohibido beber, comer y fumar dentro del centro de procesamiento de datos para así poder evitar daños en los equipos?

   Si (X) No ( )

7. ¿Existe un inventario actualizado de los equipos donde se detalle su ubicación y la persona responsable del mismo?

   Si ( ) No (X)

8. ¿Los equipos son protegidos con cubiertas plásticas o de otro material?

   Si ( ) No (X)

9. ¿Posee el centro de procesamiento de datos aire acondicionado?

   Si (X) No ( )

10. ¿Qué medidas emplean para proteger a los equipos de fallas eléctricas?

	SI	NO
• Reguladores	( )	(X)
• Sistema de energía no Interrumpido (UPS)	( )	(X)
• Fuente de energía alterna	(X)	( )

11. ¿Los cables de red y de energía están protegidos?

    Si ( ) No (X)

12. ¿Se tienen conectados a los contactos del equipo otros equipos electrónicos?

    Si (X) No ( )

13. ¿Los equipos reciben mantenimiento?

    Si (X) No ( )

14. ¿Se dispone de equipos de respaldo que puedan utilizarse en caso de contingencias?

    Si ( ) No (X)

15. ¿Existe un registro de las fallas que son reportadas por usuarios de los equipos?

    Si ( ) No (X)

16. ¿Existe un registro de los equipos, software o información que entran y salen del centro de procesamiento de datos?

    Si ( ) No (X).

17. ¿Existen alarmas contra incendios?

    Si ( ) No (X).

18. ¿Existen extintores en el centro de procesamiento de datos?

    Si (X) No ( ).

19. ¿Se tienen identificadas y señaladas las salidas de emergencia?

    Si ( ) No (X).

20. ¿Existen respaldos de backups de los archivos en dispositivos externos (CD's, DVD, USB, entre otros)

    Si (X) No ( ).

Anexo IV: EVALUACION DE SEGURIDAD LOGICA

1. ¿Cuentan con una política documentada para la gestión de las claves de acceso?

   Si ( ) No (X)

2. ¿Qué método emplean para generar las claves de acceso a los sistemas de información?

   Software (X) Elegida por el usuario ( )

3. ¿Los permisos son asignados de acuerdo a las funciones del usuario?

   Si (X) No ( )

4. ¿Se lleva un registro de los cambios de privilegios en los sistemas de información en el caso de que el usuario cambie de función dentro del centro de procesamiento de datos?

   Si ( ) No (X)

5. ¿Se bloquea el equipo después de un número limitado de ingresos de claves incorrectas?

   Si ( ) No (X)

6. ¿Se realizan seguimientos a los registros de accesos no autorizados, autorizados y fallidos?

   Si ( ) No (X)

7. ¿Es limitado el tiempo de conexión a la red al horario de oficina?

   Si ( ) No (X)

8. ¿Existen respaldos de backups de los archivos en dispositivos externos (CD, DVD, USB, entre otros)

   Si (X) No ( ).

Anexo V: EVALUACION DE SEGURIDAD EN REDES

FIREWALL

1. ¿Qué controles de acceso tiene el firewall?

   Controles sobre los equipos que tiene acceso a internet.

2. ¿Se examinan los servicios de internet que los usuarios necesitan para darles el respectivo acceso?

   Si (X) No ( )

3. ¿Se generan registros de los intentos de accesos no autorizados?

   Si ( ) No (X)

ANTIVIRUS

4. ¿Existe controles contra el uso de software malicioso (virus)?

   Si (X) No ( )

5. ¿Hay un antivirus instalado en cada equipo (incluidos el servidor) o hay un solo antivirus en toda la red?

   En cada equipo existen antivirus instalados.

6. ¿El escaneo de las maquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas?

   El encargado de sistemas.

7. ¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?

   Si ( ) No (X)

Anexo VI: CUESTIONARIO DE PREGUNTAS MECANISMOS DE SEGURIDAD DE LA INFORMACION

1. ¿Se requiere un Sistema Biométrico en el CIT, si es así con que características?

   Sí se requiere, las características serían:

   - Ingreso en edificio.
   - Ingreso a lugares autorizados
   - Con un sistema de ingreso a lugares definidos
   - Ingreso de personas autorizadas
   - Bitácora de número de veces que entran.

2. ¿En qué lugar se requiere el Sistema Biométrico?

   En el 1er Piso (horarios de ingreso y salida).
   En el 4to Piso (ingreso autorizado al Data Center).

3. ¿Se requiere de un Sistema de video vigilancia, si es así con que características?

   Sí se requiere, las características serían:

   - Ingreso y egreso de personal (interno y externo).
   - Reconocimiento facial.
   - Movimiento (infrarrojo).

4. ¿En qué lugar se requiere el Sistema de video vigilancia?

   Se requerirá de 1 videocámara por piso, la cual estaría situada al frente de cada escalera.

5. ¿Se requiere de una mejora con respecto al antivirus, firewall y Backup?

Se requiere de un antivirus corporativo que contenga estos 3 mecanismos en uno solo, con las siguientes características:

- Un antivirus que tenga un servidor central de actividades
- Que elija el mejor antivirus entre Nod32, Karpeski, Sophos, etc.
- Que lo instale a cada cliente (trabajadores de CIT).
- Contenga un Firewall (Fortinet o Demarcador).
- Se pueda hacer un Backup selectivo.
- En todo caso el Backup de la información se hace en discos duros externos.

6. ¿Se requiere de UPS (fuente de poder ininterrumpibles)?

   Sí, para cada oficina de administrativos.

7. ¿Se requiere de Sistema de detección de Humo?

   Sí, para cada oficina de administrativos.

8. ¿Se requiere de extintores?

   Actualmente se cuenta con extintores (1 por piso del tipo PQS), pero no se lleva con un registro de recargas.

Anexo VII: ESTADOS DE EMERGENCIA.

Permite identificar cuáles pueden ser los eventos que se pueden presentar que afecten el normal funcionamiento de la plataforma, afecte el ingreso de datos y la operación de los Sistemas de Información

Evento	**Descripción**	**Proceso alterno que debe realizar el usuario del sistema**	**Proceso alterno que debe realizar el personal de Sistemas**
Caída de los Sistemas	Se produce cuando: Ninguna estación de trabajo funciona, el computador no ingresa a las aplicaciones o no hay comunicación con la red; algunos de los elementos principales que impiden que la red funcione adecuadamente, pueden ser: Servidor, UPS del servidor, concentrador o Switches, puntos de red.	Mientras se restablece el sistema se debe realizar las operaciones de registro de manera manual, solicitar soporte a la Coordinación Administrativa del CIT- UNP.	Informar del problema a la Coordinación Administrativa, para asignar al personal de soporte, los mismos que identifican cuál de los elementos no está funcionando y se procede a realizar el reemplazo respectivo.
Estación de Trabajo no funciona	Se produce cuando: No hay energía en el toma corriente, cables de energía flojos o mal conectados, punto de red deteriorado, patch cord(cable de conexión) flojo en la conexión de equipo o	En la toma de energía no hay corriente eléctrica o el cable de energía esta flojo o mal conectado: Los usuarios deben verificar que estos	Verificar cada uno de los elementos que describen el problema y corregir el elemento en conflicto o reemplazarlo. La coordinación administrativa y de Soporte debe apoyar.

	la caja de punto de red, clave de acceso a la red bloqueada, problemas con el Hardware.	elementos estén bien conectados, o utilizar otra estación de trabajo disponible, solicitar soporte a la Coordinación Administrativa del CIT- UNP	
El programa o aplicación transaccional no ingresa al sistema	Se puede producir porque la conexión de red esta deshabilitada, borraron acceso directo o icono al programa, archivos de configuración del programa fueron borrados, servidor fuera de servicio.	Utilizar otra estación de trabajo para realizar sus tareas diarias sino es posible realizarlas manualmente de acuerdo a las instrucciones dadas en caída de sistemas, reportar a la Coordinación Administrativa del CIT- UNP	Verificar el caso mencionado y restaurar los elementos que están en conflicto. La coordinación administrativa y Desarrollo de Sistemas debe apoyar.
Perdida de datos en el programa o aplicación transaccional	Ocurre cuando se pierden datos de registro diario del área operativa que ingresa a las aplicaciones transaccionales para realizar las operaciones	Mientras se restablece el sistema se debe reportar a la Coordinación Administrativa del CIT-UNP.	Restauración de archivos del Backup si se realizó entre las fechas indicadas. Revisar tabla de referencia de realización de backup y las políticas de seguridad de la información.
Errores de realizar: advertencia de los	Los mensajes de error de la aplicación	Tomar nota del mensaje de error	Se debe reportar al personal de Soporte y de Desarrollo de

programas o aplicaciones transaccionales.	expresan alguna anomalía dentro de los procesos normales que se realizan, cada mensaje de error dentro de la aplicación emite un código con el que se puede identificar la causa, con el código del error que aparece en la pantalla, indica que puede estar pasando, es muy importante reconocer cual es el código de error y el mensaje completo para poder identificar y realizar el proceso de corrección de dicha tabla.	y comunicar a la Coordinación Administrativa del CIT- UNP, para que sea analizado y se establezca una posible solución. Mientras se restablece el sistema se debe realizar tareas pendientes de acuerdo al cronograma laboral.	Sistemas para saber si el error persiste y nos permite realizar o continuar con el proceso.

Anexo VIII: CRITERIOS DE RIESGO-DISPONIBILIDAD.

ACTIVOS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	PROMEDIO
[S] Servicios																																								
[telf] Telefonía Ip.	2	2	3	2	2	3	3	2	2	2	2	2	3	2	2	3	3	2	2	3	2	3	3	2	3	3	3	3	3	2	2	3	2	2	3	2	3	2	2
[inte] Internet	2	2	4	3	4	3	2	4	4	4	3	4	2	4	2	3	2	3	3	2	4	4	4	3	2	3	2	3	4	2	3	3	2	3	3	3	3	3	3
[COM]Redes de Comunicaciones																																							
[Rlan]Red LAN	2	3	3	2	2	3	2	3	2	2	2	3	3	3	3	3	2	3	2	3	2	3	2	2	2	3	2	2	3	2	2	3	2	2	3	2	2	3	2
[Rwif]Red Wifi	2	3	3	2	3	3	2	3	3	3	2	3	2	3	2	3	3	2	3	3	3	3	2	3	3	2	3	3	3	3	2	2	2	3	2	3	2	3	3
[SW] Software																																							
[Siaf]Sistema Integrado de Administración Financiera.	2	1	2	1	3	2	2	1	1	1	3	3	3	2	2	1	1	2	3	1	1	3	2	2	1	2	1	2	3	2	2	3	2	3	1	1	2	1	2
[Siga]Sistema Integrado de Gestión Académico.	1	1	1	3	2	3	1	1	2	3	2	1	2	2	1	1	1	1	2	1	1	1	2	2	2	1	2	1	1	1	2	3	2	2	1	2	3	1	2
[Sgad]Sistema de Gestión Administrativa.	3	1	2	1	1	2	2	2	1	3	2	3	3	2	2	2	2	2	3	2	3	2	2	3	2	3	1	2	2	2	2	2	2	2	2	1	1	3	2
[Stdo]Sistema de Tramite documentario.	3	3	1	3	2	2	3	1	3	3	2	3	3	2	2	1	3	1	2	2	1	2	1	1	1	2	3	2	3	1	2	1	3	1	2	3	2	1	2
[Saba]Sistema de Abastecimientos.	2	3	1	2	1	1	1	2	2	1	3	2	2	1	3	2	2	1	3	2	2	2	3	3	2	1	2	3	3	1	3	1	2	1	2	3	2	2	2
[Scap]Sistema de Control de Asistencia del personal.	2	1	1	2	1	2	2	3	2	1	1	2	1	2	3	2	1	3	2	1	2	3	2	3	2	1	3	2	3	2	3	1	2	2	1	1	3	2	2
[Sbpr]Sistema de Banco de Preguntas.	1	2	2	2	2	3	1	2	1	3	3	2	3	2	1	1	3	3	3	1	3	3	2	2	2	3	3	1	3	2	2	3	1	2	2	2	2	3	2
[Sgdo] Sistema de Gestion Docente	2	3	1	3	3	1	2	3	3	1	2	2	2	2	3	2	1	1	3	1	2	2	2	1	1	1	3	1	1	3	1	2	3	3	1	1	3	2	2
[HW] Hardware																																							
[Mimp]Medios de impresión	3	3	3	4	2	4	3	4	4	4	2	3	2	3	3	2	4	3	4	4	4	4	3	4	4	2	3	3	3	3	2	4	3	2	2	4	3	2	3
[Cesc]Computadoras de escritorio	4	2	2	4	4	4	3	4	4	4	2	2	2	3	3	4	2	2	2	2	3	3	3	4	3	3	3	2	3	4	2	4	3	2	3	2	4	2	3
[Spro]Servidor proxy	4	2	3	3	2	3	3	2	3	4	3	3	2	4	2	4	2	2	4	4	3	2	4	2	3	2	3	2	3	3	4	2	3	3	2	2	4	4	3
[MEDIA]Soportes de Informacion																																							
[Disk]Discos	2	3	3	3	3	4	2	2	3	4	2	3	2	3	4	2	3	2	3	3	3	2	4	4	3	2	4	4	4	4	3	4	4	3	4	3	3	2	3
[Musb)Memoria USB	3	4	3	3	3	3	3	3	4	3	3	3	4	4	3	4	3	4	4	4	4	3	4	4	4	4	3	4	3	4	4	4	3	3	4	3	3	4	4
[AUX]Equipamiento Auxiliar																																							
[Sain]Sistema de alimentación ininterrumpida	4	4	4	4	4	4	3	4	4	3	3	4	3	3	4	3	4	4	4	4	3	3	3	3	4	3	4	3	3	4	4	4	4	4	3	3	4	4	4
[L]Instalaciones																																							
[Edif]Edificio	2	3	2	3	4	4	3	4	2	2	3	4	2	3	4	4	2	3	2	3	3	4	2	3	3	4	3	3	4	3	2	2	3	2	4	3	2	3	3
[P]Personal																																							
[User]Usuarios Finales	3	4	2	3	4	3	2	4	3	3	2	3	2	4	3	4	4	2	2	3	2	4	4	4	4	2	2	4	4	2	3	4	4	2	2	4	3	3	3

Anexo IX: CRITERIOS DE RIESGO -INTEGRIDAD.

ACTIVOS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	PROMEDIO
[S] Servicios																																								
[telf] Telefonía Ip.	1	3	1	2	2	1	1	1	3	3	1	2	2	3	2	1	2	3	1	3	1	3	3	3	3	3	1	3	3	2	2	2	3	1	2	1	2	3	2
[inte] Internet	2	1	3	3	1	1	1	1	1	1	1	1	2	3	2	1	3	3	1	1	2	1	3	2	1	3	3	1	2	1	2	2	3	2	3	2	2	3	2
[COM]Redes de Comunicaciones																																							
[Rlan]Red LAN	2	1	3	3	2	3	2	2	3	1	3	1	2	1	3	1	2	3	1	3	2	3	1	3	1	2	1	2	1	1	1	1	1	1	3	3	1	1	2
[Rwif]Red Wifi	2	4	4	2	2	4	2	2	3	4	2	4	3	4	4	3	3	2	3	2	4	3	4	3	4	4	2	4	3	2	3	2	4	3	4	3	2	3	3
[SW] Software																																							
[Siaf]Sistema Integrado de Administración Financiera.	2	2	2	3	2	1	2	1	2	1	1	2	3	2	3	2	3	3	2	2	2	2	3	1	3	2	2	1	3	1	2	2	1	1	3	1	2	3	2
[Siga]Sistema Integrado de Gestión Académico.	2	2	2	2	3	3	1	1	1	1	3	1	2	3	3	1	3	3	2	3	3	2	1	2	3	3	2	3	1	3	1	3	3	2	3	1	1	3	2
[Sgad]Sistema de Gestión Administrativa.	3	1	3	2	1	2	3	3	1	2	2	3	2	2	2	1	2	3	3	3	2	2	3	2	1	2	3	2	3	3	2	2	3	1	1	1	2	1	2
[Stdo]Sistema de Tramite documentario.	2	3	3	1	1	2	3	3	3	3	1	3	3	2	3	1	3	1	3	3	1	1	1	3	3	3	3	2	2	1	2	3	2	2	1	3	3	2	2
[Saba]Sistema de Abastecimientos.	1	1	1	2	1	1	3	3	2	2	3	2	2	3	3	2	1	2	3	2	2	1	3	2	1	3	2	3	2	3	1	1	1	3	3	2	1	3	2
[Scap]Sistema de Control de Asistencia del personal.	2	3	2	2	1	1	2	2	3	2	2	1	1	1	2	2	2	3	1	2	3	3	2	1	3	1	1	1	3	1	1	2	2	3	2	1	2	1	2
[Sbpr]Sistema de Banco de Preguntas.	3	3	3	3	2	3	3	3	3	2	3	2	1	3	1	1	1	3	2	2	2	2	2	3	2	1	2	3	3	2	3	2	3	1	1	2	2	1	2
[Sgdo] Sistema de Gestion Docente	2	3	3	1	2	1	1	1	1	2	3	2	3	2	3	1	2	1	3	3	1	1	3	1	3	3	2	1	2	1	3	1	2	1	3	2	2	2	2
[HW] Hardware																																							
[Mimp]Medios de impresión	3	4	2	1	2	1	1	2	3	3	4	4	4	3	1	1	1	4	1	4	2	2	3	2	4	4	4	4	4	1	1	4	3	2	2	1	2	4	3
[Cesc]Computadoras de escritorio	4	2	3	2	4	3	1	2	2	3	1	2	2	2	2	2	4	3	1	4	3	1	3	4	1	2	3	1	1	4	2	2	1	2	3	4	3	4	2
[Spro]Servidor proxy	1	3	3	4	2	2	3	2	3	1	4	2	1	3	1	1	2	2	2	3	4	4	1	3	2	2	2	4	2	1	2	2	1	4	4	3	2	4	2
[MEDIA]Soportes de Informacion																																							
[Disk]Discos	2	2	2	1	2	1	1	2	2	1	1	1	2	1	1	1	1	2	2	2	2	2	1	2	2	2	1	2	2	1	2	2	1	1	2	2	2	1	2
[Musb)Memoria USB	3	3	4	3	3	4	4	3	3	4	3	4	3	3	3	3	3	3	3	4	3	4	4	4	4	4	4	4	4	4	4	4	3	3	4	3	4	4	4
[AUX]Equipamiento Auxiliar																																							
[Sain]Sistema de alimentación ininterrumpida	3	3	4	3	4	4	3	4	4	4	3	4	3	3	4	3	3	3	4	3	4	3	3	3	3	3	4	4	4	3	4	4	3	3	4	4	4	3	3
[L]Instalaciones																																							
[Edif]Edificio	2	4	3	4	2	2	3	2	2	2	3	3	2	2	4	3	4	3	4	2	4	4	4	3	3	4	4	2	3	2	2	2	2	4	2	2	3	3	3
[P]Personal																																							
[User]Usuarios Finales	3	2	2	3	4	3	4	3	3	4	3	2	2	2	2	3	2	4	2	3	4	3	4	3	2	4	4	2	4	2	2	2	4	4	2	3	4	2	3

Anexo X: CRITERIOS DE RIESGO -CONFIDENCIALIDAD.

ACTIVOS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	PROMEDIO
[S] Servicios																																							
[telf] Telefonía Ip.	3	3	2	3	1	2	1	2	3	1	2	2	3	2	2	3	2	3	1	3	1	1	2	2	2	3	2	3	3	2	3	2	1	2	1	1	3	1	2
[inte] Internet	2	2	3	3	2	3	2	4	4	3	3	2	4	3	2	3	4	4	2	4	2	3	4	2	3	2	4	2	2	4	3	2	2	4	4	3	3	2	3
[COM]Redes de Comunicaciones																																							
[Rlan]Red LAN	3	1	2	1	3	1	2	2	1	1	2	1	1	1	3	3	2	2	2	2	3	2	2	2	3	2	3	1	2	2	2	2	3	1	3	2	2	1	2
[Rwif]Red Wifi	2	3	4	4	2	3	3	3	2	2	2	2	3	2	2	2	2	2	3	2	3	2	3	3	3	3	2	2	2	3	2	2	2	2	3	2	3	3	3
[SW] Software																																							
[Siaf]Sistema Integrado de Administración Financiera.	1	3	3	1	1	3	2	1	2	3	1	3	3	1	2	3	2	2	1	2	3	2	3	3	3	3	3	2	1	1	3	3	2	1	2	3	3	3	2
[Siga]Sistema Integrado de Gestión Académico.	2	1	2	3	3	3	3	3	3	3	3	2	1	3	2	3	2	1	2	3	2	3	1	1	2	2	1	3	2	3	2	1	3	1	1	1	1	3	2
[Sgad]Sistema de Gestión Administrativa.	1	2	1	3	3	1	3	2	3	3	3	3	3	2	2	3	2	1	2	3	2	3	2	1	2	2	3	2	1	2	3	3	2	1	3	1	1	2	2
[Stdo]Sistema de Tramite documentario.	1	3	1	3	3	2	3	2	1	2	2	3	1	2	2	1	1	1	1	2	1	3	2	1	1	3	2	2	3	2	3	3	2	3	2	1	1	3	2
[Saba]Sistema de Abastecimientos.	2	1	3	2	3	1	1	3	3	3	3	3	2	1	1	2	2	2	1	1	1	1	3	2	3	2	1	3	2	1	2	2	1	2	1	2	2	1	2
[Scap]Sistema de Control de Asistencia del personal.	3	2	3	1	2	3	1	3	1	2	1	2	1	1	1	1	1	2	2	1	2	3	2	3	2	2	1	1	3	3	2	2	3	2	1	3	3	3	2
[Sbpr]Sistema de Banco de Preguntas.	2	1	2	1	1	2	2	1	3	1	2	3	3	1	1	3	2	3	2	3	1	1	3	2	1	2	1	2	1	1	1	3	3	3	2	2	2	1	2
[Sgdo] Sistema de Gestion Docente	2	2	3	2	1	1	2	1	1	3	1	2	2	3	2	2	2	3	1	3	1	2	3	2	3	2	2	3	1	2	2	1	2	3	2	3	2	1	2
[HW] Hardware																																							
[Mimp]Medios de impresión	4	4	4	3	3	4	4	3	4	3	4	3	3	3	4	4	4	4	4	4	3	3	4	3	4	3	4	4	3	3	3	3	3	3	3	4	3	4	4
[Cesc]Computadoras de escritorio	3	3	4	4	3	3	4	4	3	3	4	4	3	4	3	3	3	4	4	3	3	3	4	4	4	3	3	4	3	4	3	4	4	4	3	3	4	4	4
[Spro]Servidor proxy	3	4	4	4	4	3	4	3	3	3	3	4	4	3	3	4	3	4	4	3	3	4	4	4	3	4	3	4	3	4	3	4	3	3	4	3	4	4	4
[MEDIA]Soportes de Informacion																																							
[Disk]Discos	3	2	4	3	3	4	4	4	3	4	2	3	3	4	3	3	2	4	2	4	4	3	2	2	3	3	3	4	2	2	3	4	4	2	2	2	4	3	3
[Musb)Memoria USB	3	4	4	3	3	4	4	3	4	4	3	3	3	3	4	4	4	4	3	4	3	3	3	4	3	3	4	4	4	3	4	4	4	4	3	4	4	4	4
[AUX]Equipamiento Auxiliar																																							
[Sain]Sistema de alimentación ininterrumpida	4	4	3	3	4	3	4	3	4	4	3	4	3	4	3	4	3	3	4	4	4	4	3	4	4	3	3	4	3	4	4	3	4	3	3	3	4	4	4
[L]Instalaciones																																							
[Edif]Edificio	3	4	4	3	2	3	3	2	4	3	2	4	4	2	2	4	3	4	2	2	3	4	3	3	2	2	2	3	4	4	2	2	2	3	3	2	2	4	3
[P]Personal																																							
[User]Usuarios Finales	2	2	4	2	2	2	2	2	2	2	2	2	3	4	2	3	3	3	3	4	3	3	4	4	2	2	3	4	2	3	3	2	4	2	4	4	4	2	3

Anexo XI: CRITERIOS DE RIESGO -AUTENTICIDAD.

ACTIVOS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	PROMEDIO
[S] Servicios																																							
[telf] Telefonía Ip.	3	2	2	3	2	3	3	3	3	3	3	2	2	3	3	2	2	3	3	2	2	2	3	2	2	2	3	2	2	3	3	3	2	3	3	3	2	2	3
[inte] Internet	2	2	4	2	4	3	3	3	2	2	3	4	3	3	4	4	3	4	2	2	3	4	3	2	4	3	4	2	4	2	3	2	3	3	2	3	4	3	3
[COM]Redes de Comunicaciones																																							
[Rlan]Red LAN	2	2	3	2	2	2	2	3	3	3	2	2	3	2	3	2	2	3	3	3	3	2	2	2	3	3	3	3	3	3	2	2	3	2	2	2	2	3	2
[Rwif]Red Wifi	3	3	3	2	2	3	2	3	3	3	3	2	3	3	2	3	3	3	3	2	3	2	3	3	2	3	2	2	3	3	2	2	2	2	2	2	3	2	3
[SW] Software																																							
[Siaf]Sistema Integrado de Administración Financiera.	1	1	3	1	1	1	3	2	3	1	3	1	1	3	3	1	3	2	2	3	2	1	2	3	2	1	1	3	2	2	2	3	3	2	2	3	3	1	2
[Siga]Sistema Integrado de Gestión Académico.	1	1	3	2	2	1	1	3	2	1	1	3	1	2	1	2	2	3	2	3	3	1	2	2	3	1	2	2	1	2	2	3	1	1	1	3	3	3	2
[Sgad]Sistema de Gestión Administrativa.	3	3	2	1	3	1	1	1	3	3	3	2	2	1	1	2	2	2	3	3	1	3	2	1	2	1	2	2	2	2	1	2	3	2	1	1	3	3	2
[Stdo]Sistema de Tramite documentario.	2	2	2	1	2	2	3	3	2	3	1	3	2	3	2	2	2	3	1	1	3	2	2	1	2	3	3	3	2	3	1	2	2	3	2	1	3	3	2
[Saba]Sistema de Abastecimientos.	3	2	1	2	2	2	1	3	3	2	2	1	3	3	2	3	3	2	3	1	2	2	3	1	3	1	3	2	3	3	1	2	3	3	1	3	2	2	2
[Scap]Sistema de Control de Asistencia del personal.	1	2	2	1	3	3	1	1	3	2	2	2	3	2	1	2	1	3	3	2	1	1	3	3	3	2	1	1	1	3	1	3	3	2	2	2	3	3	2
[Sbpr]Sistema de Banco de Preguntas.	1	1	3	3	1	1	2	2	2	2	2	3	3	2	2	3	3	3	3	2	1	1	3	1	3	2	1	2	1	2	2	1	1	2	2	1	3	1	2
[Sgdo] Sistema de Gestion Docente	3	3	1	1	3	2	3	3	3	1	1	2	1	2	3	1	3	1	3	3	2	2	3	1	1	1	1	3	3	3	2	1	3	1	1	3	1	2	2
[HW] Hardware																																							
[Mimp]Medios de impresión	4	3	3	3	2	4	4	2	2	3	2	2	2	3	3	2	3	3	4	3	4	2	3	3	3	3	3	4	4	4	4	3	2	3	3	4	4	4	3
[Cesc]Computadoras de escritorio	2	3	3	3	4	3	2	2	4	4	3	3	2	4	4	4	4	4	4	2	2	4	4	2	4	2	4	4	3	4	2	4	3	2	2	4	2	4	3
[Spro]Servidor proxy	3	3	4	2	4	4	3	3	4	2	3	3	3	4	3	4	3	3	2	4	2	2	2	3	4	3	2	4	2	2	4	3	3	2	2	4	2	2	3
[MEDIA]Soportes de Informacion																																							
[Disk]Discos	4	3	3	4	3	2	4	4	4	3	2	3	3	4	3	4	2	2	3	2	4	2	3	4	3	2	4	3	4	4	4	4	4	3	3	3	4	2	3
[Musb)Memoria USB	3	3	4	3	4	4	4	3	4	4	4	4	3	4	4	4	3	3	4	4	4	4	4	4	3	3	4	3	3	4	3	4	4	4	3	3	3	3	4
[AUX]Equipamiento Auxiliar																																							
[Sain]Sistema de alimentación ininterrumpida	4	3	4	4	3	4	4	3	4	3	4	3	4	3	3	4	4	4	3	4	3	4	3	3	4	4	3	4	3	4	3	4	4	4	3	4	4	4	4
[L]Instalaciones																																							
[Edif]Edificio	2	4	2	2	2	4	2	4	2	2	4	2	2	3	2	3	4	3	4	4	2	4	3	3	3	3	4	3	3	4	4	4	3	3	3	2	3	2	3
[P]Personal																																							
[User]Usuarios Finales	2	2	3	3	4	4	2	3	3	2	2	4	3	3	3	2	3	2	2	3	3	4	3	3	4	3	2	3	3	3	4	4	4	2	4	3	3	2	3